THE GROWING CYBER THREAT
p36

BRIEFING
COMPUTER SECURITY
p59

Technology Review

PUBLISHED BY MIT SINCE 1899

Can AIDS Be Cured?

A RADICAL NEW APPROACH SUGGESTS MAYBE p44

How China Became the World's Solar Leader
p52

Buzz Aldrin: Let's Go to Mars
p26

The iPad Hacked Open
p78

Which Countries Have the Fastest Broadband?
p24



$4.99
08
0 71486 01308 2

The Authority on the Future of Technology
August 2010
www.technologyreview.com

technology
review
Published by MIT

This PDF is for your personal, non-commercial use only.
Distribution and use of this material are governed by copyright law.
For non-personal use, or to order multiple copies please email
permissions@technologyreview.com.

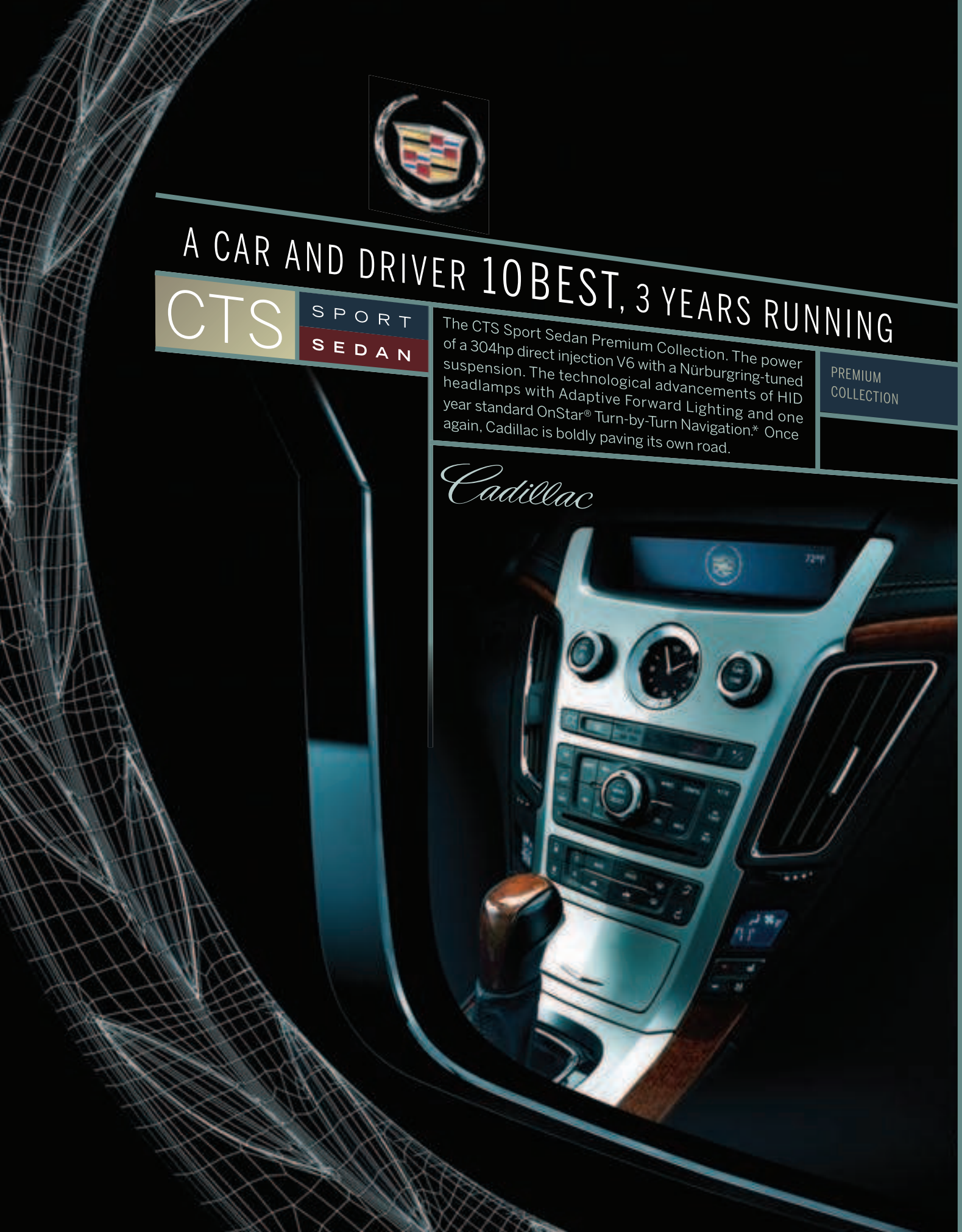
A CAR AND DRIVER 10BEST, 3 YEARS RUNNING

CTS SPORT SEDAN

The CTS Sport Sedan Premium Collection. The power of a 304hp direct injection V6 with a Nürburgring-tuned suspension. The technological advancements of HID headlamps with Adaptive Forward Lighting and one year standard OnStar® Turn-by-Turn Navigation.* Once again, Cadillac is boldly paving its own road.

PREMIUM COLLECTION

Cadillac





CADILLAC.COM

*Visit onstar.com for coverage map, details and system limitations. Services vary by model and conditions. ©2010 General Motors. Cadillac® CTS® Nürburgring®






Celebrating ten years of bringing together the brightest minds and most innovative ideas.

Now in its 10th year, EmTech@MIT brings Technology Review's mission to life by showcasing the most important emerging technologies and explaining their impact. The annual conference spotlights technological innovations that are changing the face of business and driving the global economy.

Spanning IT to energy, the Web to biomedicine and materials, the editors of Technology Review have pinpointed the key technologies that will drive the economy forward. **REGISTER NOW!**

Why do you need to attend EmTech@MIT 2010?

- To discover key emerging technologies in IT, energy, the Web, biomedicine, and materials
- To understand how up-and-coming trends in these areas are going to impact your business
- To network with leaders in business and technology, including CEOs, CTOs, CIOs, policy leaders, entrepreneurs, venture investors, and more.

Register Now and Save!

Technology Review subscribers receive an additional 10% off of any full-conference package! Special discount for *Technology Review* subscribers!

Interested in Sponsoring?

Each year, EmTech@MIT attracts top decision makers from the technology, engineering, investment, and management communities. Partnering with Technology Review allows you to showcase your company's technologies and capabilities to our influential audience. E-mail **sponsorship@technologyreview.com** to learn more.

Sponsors

Alcatel·Lucent

Sprint

Partners

MIT ENTERPRISE FORUM

mITX MASSACHUSETTS INNOVATION & TECHNOLOGY EXCHANGE WHAT'S NEXT.



EmTech@MIT 2010

10th Anniversary Event! MIT Campus - Cambridge, MA • September 21-23, 2010

The 2010 conference is packed with world-renowned keynotes, cutting edge demos, compelling panel discussions, and opportunities for exclusive networking with our senior-level audience.



Nazeer Bhore
Senior Technology Advisor, ExxonMobil



Dan Hesse
CEO, Sprint



Scott Elrod
VP and Director of the Hardware Systems Laboratory, PARC



Ellen Williams
Chief Scientist, BP



Kris Gopalakrishnan
CEO, Infosys Technologies



Stephen Wolfram
CEO, Wolfram Research



Christine Herron
Principal, First Round Capital

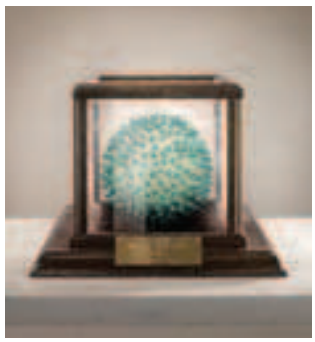


Robert J. Zimmer
President, University of Chicago

Check out the 2010 speaker lineup and register online at: **www.technologyreview.com/emtech**

Register by July 31st and save $400!

Enter code **TRSub** on Step 2 when registering online at
www.technologyreview.com/reg1.



COVER
Photo illustration by Jana Leon

36 Moore's Outlaws
The growing threat of cyber crime, espionage, and warfare.
By DAVID TALBOT

www.technologyreview.com/cybersecurity Watch a video about worsening security and the risk of cyber war.

44 Can AIDS Be Cured?
Researchers are pursuing radical new strategies to eliminate HIV from the body.
By JON COHEN

52 Solar's Great Leap Forward
Suntech CEO Zhengrong Shi made China a powerhouse in photovoltaics. Now he plans to make solar power as cheap as conventional electricity.
By KEVIN BULLIS

www.technologyreview.com/suntech Hear the CTO of Suntech explain the company's advanced solar technology.

8 **Letters**
10 **From the Editor**

NOTEBOOKS

12 **Militarizing Cyberspace**
To preserve the open Internet, we must stop the cyber arms race. *By Ronald Deibert*

12 **Preventing HIV**
We should treat high-risk populations before they have been exposed. *By Robert Grant*

14 **Photovoltaics Come of Age**
Solar panels are cheap enough to become a major component of green energy. *By Ken Zweibel*

TO MARKET

17–22 **Technology Commercialized**
A robot to help with weight loss, personal AC, solar recharger, portable hotspot, pocket-sized bomb detector, electric delivery vehicle, and more.

GRAPHITI

24 **The Global Broadband Spectrum**
A detailed chart shows which countries have fast broadband and which don't. *By Tommy McCall and Matt Mahoney*



Q&A

26 **Buzz Aldrin**
The Apollo astronaut says: forget the moon, let's colonize Mars.
By Brittany Sauser



PHOTO ESSAY

28 **Robot in the OR**
The da Vinci robot can shorten surgical recovery times.
By Emily Singer

BRIEFING

59–70 **Computer Security**
Cyber attacks are inspiring new defenses for networks, personal computers, and smart phones.

REVIEWS

72 **America's Broadband Dilemma**
The FCC aims to bring the country's Internet access up to speed.
By Bobbie Johnson

74 **The Argument over Aging**
A drug to slow the decline is on the horizon, some researchers say. Others don't believe it.
By Karen Weintraub

76 **The German Experiment**
A decade ago, the German government set a premium price on alternative power sources.
By Evan I. Schwartz

HACK

78 **iPad 3G**
A peek inside the tablet reveals how it connects to the world.
By Erica Naone

www.technologyreview.com/hack See an interactive version.



28

DEMO

80 **Inexpensive, Unbreakable Displays**
Researchers at Hewlett-Packard are making silicon electronics on rolls of plastic. The result could be flexible, cheap displays. *By Katherine Bourzac*

■ **www.technologyreview.com/demo** Watch a video of HP's printing process in action.



FROM THE LABS

84 **Materials**
85 **Information Technology**
86 **Biomedicine**

26 YEARS AGO IN *TR*

88 **The Long Fight Ahead**
When researchers found the cause of AIDS in the early 1980s, their work had only just begun. *By Matt Mahoney*

Can tactile computing prevent a car accident?

Find the latest computing research in IEEE *Xplore*

Wherever you find the most advanced computing technology, chances are you'll find the IEEE *Xplore* digital library. That's because IEEE *Xplore* is filled with cutting-edge research—from software engineering and parallel architecture, to tactile computing that can help you avoid a car accident.

When it comes to computing, the research that matters is in IEEE *Xplore*.

See for yourself. Read "Tactile and Multisensory Spatial Warning Signals for Drivers," only in IEEE *Xplore*.

Try IEEE *Xplore* free—
visit www.ieee.org/preventingaccidents

IEEE *Xplore*® Digital Library
Information driving innovation

IEEE

Technology
PUBLISHED BY MIT Review

Editor in Chief and Publisher
Jason Pontin

EDITORIAL

Editor
David Rotman

Art Director
Lee Caulfield

Chief Correspondent
David Talbot

Senior Editor, MIT News
Alice Dragoon

Senior Editor, Biomedicine
Emily Singer

Senior Editor, Special Projects
Stephen Cass

Computing Editor
Tom Simonite

Energy Editor
Kevin Bullis

Materials Science Editor
Katherine Bourzac

Copy Chief
Linda Lowenthal

Copy Editor
Timothy Maher

Research Editor
Matt Mahoney

Assistant Editor
Erica Naone

Editorial Assistant
Kristina Grifantini

Assistant Designer
Angela Tieri

Production Director
James LaBelle

Contributing Editors
Simson Garfinkel
Mark Williams

TECHNOLOGYREVIEW.COM

Vice President, Online
David Foucher

Managing Editor
Will Knight

Design Director
Conrad Warre

Senior Web Producer
Brittany Sauser

Web Developers
Michael Callahan
Shaun Calhoun
Sarah Redman

CORPORATE

Chief Financial Officer
Rick Crowley

Chief Operating Officer
James Coyle

Chief Strategy Officer
Kathleen Kennedy

Executive Assistant
Leila Snyder

Manager of Information Technology
Colby Wheeler

Office Representative
Linda Cardinal

MARKETING

Manager, Marketing and Events
Amy Lammers

Associate Manager, Advertising Operations
David A. Schmidt

Associate Art Director, Marketing and Custom Publishing
Andrew Memmelaar

CONSUMER MARKETING

Vice President of Circulation and Consumer Marketing
Heather Holmes

Fulfillment Manager
Tina Bellomy

FINANCE

Accountants
Letitia Trecartin
Tim Curran

BOARD OF DIRECTORS

Reid Ashe
Judith M. Cole
Jerome I. Friedman
Theresa M. Stone
Sheila E. Widnall
Ann J. Wolpert

De Technologia non multum scimus. Scimus autem, quid nobis placeat.

CUSTOMER SERVICE AND SUBSCRIPTION INQUIRIES

National: 800-877-5230
International: 818-487-2088
E-mail: technologyreview@pubservice.com
www.technologyreview.com/customerservice
MIT Records: 617-253-8270 (alums only)
Permissions: Jennifer Martin
jmartin@wrightsreprints.com
877-652-5295, ext. 104

ADVERTISING SALES

Midwest Sales Director and National Print Strategist
Maureen Elmaleh
maureen.elmaleh@technologyreview.com
303-975-6381

West Coast Sales Director and National Digital Strategist
Patrick Viera
patrick.viera@technologyreview.com
415-659-2982

New York and Northeast
Johanna Zottarelli-Duffe
jo.duffe@technologyreview.com
857-998-9241

New England, Detroit, and Canada
Barry Echavarria
barry.echavarria@technologyreview.com
603-924-7586

Mid-Atlantic and Southeast
Clive Bullard
cbullards@cs.com
845-231-0846

Northwest
Steve Thompson
stevet@mediacentricinc.com
415-435-4678

Europe
Anthony Fitzgerald
mail@afitzgerald.co.uk
44-1488-680623

France
Philippe Marquezy
philippe.marquezy@espacequadri.com
33-1-4270-0008

Germany
Michael Hanke
michael.hanke@heise.de
49-511-5352-167

China
RP Soong
rpsoong@mittrchinese.com
010-8280-9083

India
Aninda Sen
anindas@cybermedia.co.in
91-80-43412000

Japan
Shigeru Kobayashi
shig-koby@media-jac.co.jp
813-3261-4591

Spain and South America (Online)
Pedro Moneo Laín
pedro.moneo@opinno.com
34-667-732-894

International Licensing Consultant
Chander Rai

Advertising Services
webcreative@technologyreview.com
617-475-8004

Media Kit
www.technologyreview.com/media

Technology Review
One Main Street, 7th Floor
Cambridge MA 02142
Tel: 617-475-8000
Fax: 617-475-8043

TECHNOLOGY REVIEW, INC., identifies emerging technologies and analyzes their impact for technology leaders. Technology Review publishes *Technology Review* magazine (the oldest technology magazine in the world, founded in 1899) and the daily website TechnologyReview.com; it also produces live events such as the EmTech Conference. Technology Review is an independent media company owned by the Massachusetts Institute of Technology. The views expressed in our various publications and at our events are often not shared by MIT.



lead innovation

Technology Innovation for Intelligence Dominance

The National Reconnaissance Office **Director's Innovation Initiative (DII) Program** nurtures innovative concepts and creative ideas to transform intelligence to revolutionize systems and capabilities for future intelligence needs. The program funds the brightest minds, best ideas, and break through technology from individuals in industry, academia, national laboratories, and other U.S. government agencies. Log onto the DII website for proposal guidance, frequently asked questions, history, and BAA and GSSA requirements.

DII research funding supports cutting-edge scientific research in a high-risk, high-payoff environment.

http://dii5.westfields.net

GRADING OUR PREDICTIONS

I always enjoy reading the new-technologies article ("10 Emerging Technologies 2010," May/June 2010). It would be interesting to see how well your predictions over the years have done. What percentage are on track? Do you do better in certain fields? If it turns out you are good at this, maybe you could sell your picks.

Ed Macho
Hilton Head Island, SC



May/June '10

While we haven't formally looked at how well our predictions have done, we may do so in the future. Thanks for the suggestion! —Editors

DREAMS OF THE FUTURE

I find every issue of *Technology Review* useful in more ways than one. First, it's always provocative reading. Second, it provides ample material to inspire my boys with technological dreams of the future: OLED lights, 3-D smart phones, jet packs, renewable solar fuels, green concrete, and implantable electronics, to name a few. And to top it off, a novel chart of U.S. energy flows that I will be using in the next lecture for my global-warming class.

David Lea
Santa Barbara, CA

CHINA AND THE WEB

As a Beijing-based tech entrepreneur and blogger at Digicha.com, I thought David Talbot's "China's Internet Paradox" (May/June 2010) was one of the best articles I've read about the subject. Public opinion on the Internet has made a difference, from the revelation of the corrupt Nanjing official to the acquittal of Deng Yujiao. But its impact can be overstated. I haven't seen evidence that online discussions have changed any major policies. Nor have they led to investigations of anyone other than marginal officials. Also, the impact of Google's partial withdrawal from China may not have had as much of an effect as we think on Chinese residents. In fact, to many Chinese users, the "War of Internet Addiction" video, which satirizes the regulatory battles over the approval of World of Warcraft and the government's 2009 attempts to "cure" Internet addiction, probably had more of an impact.

Bill Bishop
Beijing, China

THE IMPACT OF E-BOOKS

There's a lot wrong with your review of e-book readers ("Going Out of Print," May/June 2010), beginning with the assumption that print will go the way of the CD. According to a PricewaterhouseCoopers survey published by the *Financial Times* on February 9, the impact of e-readers is expected to rise in the United States from about 1 percent of sales in 2008 to about 6 percent in 2013. Books and music are not analogous. The traditional publishing industry is beset by many woes, including its inability to agree upon a digital strategy, but the e-reader is not the chief culprit. I discussed the plight of the publishing industry and its probable outcome in a recent issue of the *New York Review of Books.*

Jason Epstein
New York, NY

The author is the creator of the trade paperback and cofounder of the New York Review of Books. *—Editors*

www I agree that newspapers and magazines could profit by offering professional design and writing, but books may be different. It is much easier to self-publish today than ever before, but publishers still offer professional editing, art, and marketing, and I'm not sure how a self-published author would obtain those services. And if costs of materials, printing, and shipping are reduced through digital publishing, do publishers really lose money at $9.99?

mwilson1962
(Mark Wilson, Rochester, NY)

Publishers will only survive if they evolve their business model instead of forcing Amazon to charge more than $9.99 for Kindle books. These publishers are rushing blindly down the same path as the recording industry, maintaining an outmoded business model. The resulting piracy will be devastating to agents, publishers, and, worse, authors.

rttedrow
(Richard Tedrow, Bethesda, MD)

U.S. COMPETITIVENESS

Good Q&A with Paul Otellini (May/June 2010). He should be commended for bringing up the decline of innovation. However, I take issue with his assertion that U.S. corporate tax rates are among the highest of developed countries. After all the tax breaks and generous loopholes, the tax rate for U.S. corporations is among the lowest in the developed world.

outsider
(Subramani Iyer, San Jose, CA)

Otellini scratches the surface of problems facing U.S. companies. When I started in business years ago, government-funded research could be counted on, but for the last decade we've been ruled by those interested in gaming financial systems rather than supporting competitiveness. Corporate execs increase short-term profits by outsourcing jobs to foreign countries. Most of the competent engineers I've known employed by U.S. companies were let go in their 50s, when they can be most productive in creating the next generations of technologies.

fiberman
(Jim Hayes, Fallbrook, CA)

JOIN THE DISCUSSION, OR CONTACT US

technologyreview.com/community
E-mail letters@technologyreview.com
Write *Technology Review*, One Main Street, 7th Floor, Cambridge, MA 02142
Fax 617-475-8043
Please include your address, telephone number, and e-mail address. Letters may be edited for both clarity and length.

Tomorrow's business tools at your fingertips.



Visit Technology Review's **"Office of the Future"** Special Report to learn about the technologies that will power the office of tomorrow.

www.technologyreview.com/ootf

Technology Review
PUBLISHED BY MIT

Sponsored By

HIT PRINT INTELLIGENTLY

hp



On Risk

HOW SHOULD TECHNOLOGISTS THINK ABOUT PRECAUTIONS?

I have been thinking about risk.

As I write this column in early June, British Petroleum is still struggling to contain its leaking well in the Gulf of Mexico. After the company's drilling rig, Deepwater Horizon, exploded on April 20, as many as 19,000 barrels of oil (or as much as 800,000 gallons) spewed into the Gulf every day. A cap is now capturing a little more than 400,000 gallons a day. It is the worst environmental disaster in the history of the United States, but there may be no solution until BP completes two "relief wells" in August.

In this issue of *Technology Review*, David Talbot writes about the increasing incidence of cyber crime and espionage, and the real (if still speculative) risk of outright cyber warfare. In "Moore's Outlaws" *(p. 36)*, he quotes Stewart Baker, the former general counsel of the National Security Agency and a former policy chief at the U.S. Department of Homeland Security: "What we've been seeing, over the last decade or so, is that Moore's Law is working more for the bad guys than the good guys. It's really 'Moore's outlaws' who are winning this fight. Code is more complex, and that means more opportunity to exploit the code. There is more money to be made in exploiting the code, and that means there are more and more sophisticated people looking to exploit vulnerabilities. If you look at things like malware found, or attacks, or the size of the haul people are pulling in, there is an exponential increase."

Talbot describes experts' concerns that computer viruses have made millions of machines into "enslaved armies"—botnets—awaiting instruction by malefactors. In the days leading up to April 1, 2009, a worm called Conficker was expected to receive an update from its unknown creator, but no one knew what: "A tweak to Conficker's code might cause the three million or so machines ... to start attacking the servers of some company or government network, vomit out billions of pieces of spam, or just improve the worm's own ability to propagate." It's scary stuff.

In the first case, a complex system of technologies (whose purpose is to extract crude oil five miles under the ocean's surface) failed; in the second, a more complex system (a global computer network whose purposes are incomprehensibly various, but upon which our technological civilization depends) is failing. These failures are not so much predictable as *unsurprising*. We expanded our use of vulnerable technologies, because we were dependent upon them. How should we think about the risks inherent in technologies, particularly new technologies?

One possible intellectual tool, popular with environmentalists and policy makers, is the Precautionary Principle, which states that when something is suspected of being harmful, the burden of proof that the thing is *not* harmful rests with its proponents. This principle has a stronger and a weaker formulation. The stronger calls for regulation of any potentially harmful activity, or refraining from action altogether, until there is consensus that it is safe. The weaker does not demand regulation or bans; it weighs costs against likelihoods. The former says, "Better safe than sorry"; the latter, "Be prepared."

Although a handful of international agreements have endorsed the strong formulation, and while it possesses a quasi-legal status in European Union law, it is in fact seldom applied. (A notable exception is in the management of global fisheries.) Certainly, governments, corporations, and individuals routinely ignore it when thinking about new technologies. That's because the idea is "paralyzing," according to Cass Sunstein, the administrator of the White House Office of Information and Regulatory Affairs (and for many years a professor of law at the University of Chicago, where he wrote about behavioral economics and risk). No one knows how new technologies will be used in the future. There is *never* any consensus about risks. Crises accompany the development of any new, complex system, but their exact form tends to take us by surprise.

But if the strong formulation of the Precautionary Principle is paralyzing, the weak formulation is almost no help at all. It provides little guidance for thinking about unlikely but potentially catastrophic risks. We need an entirely *new* principle that will guide our investment in precautionary technology. When a technology fails or is unsustainable, we should be rationally confident that a fix or alternative exists or will exist, because ingenious humans have devised other technologies that will mitigate the crisis or stand in the outmoded technology's place. Government has a justified role in requiring such precautionary investment in new technologies.

In the absence of a new principle, we have mere optimism.

David Talbot's feature, which accepts that we're not likely to build an entirely new, more secure Internet, describes research into new technologies that may make our networks safer. For now, perhaps that's the best risk management we can expect. Read about them, and write and tell me what you think at jason.pontin@technologyreview.com. *—Jason Pontin*

MARK OSTOW



Find out

with *Technology Review.*

And find out first. Our writers and editors have uncommon access and expertise. Join them as they identify tomorrow's stars and explore the possibilities their technologies will bring.

Technology Review is the authority on the future of technology.



Subscribe

Start your subscription to *Technology Review* at the exclusive low rate of just $24.95 for one full year (6 issues), a 36% savings off the regular price. With your paid subscription, you will also receive free extensive access to *Technology Review*'s online archives. If you decide to cancel your subscription, simply write "Cancel" on the invoice, return it and owe nothing. No matter what you decide, the free trial issue is yours to keep.

Call **1 800 877 5230** to start your subscription now —or subscribe at **http://www.trsub.com/july**

NOTEBOOKS

Expert opinion



SECURITY

Militarizing Cyberspace

TO PRESERVE THE OPEN INTERNET, SAYS RONALD DEIBERT, WE MUST STOP THE CYBER ARMS RACE.

It has become fashionable these days to express skepticism about "cyber war"—and for good reason. The concept is ill defined; it has been used to describe everything from defacing websites to attacking critical infrastructure to committing espionage over computer networks. More troubling is that many of the heralds of cyber war have a commercial stake in the cyber security market. Some may have more ulterior motives for ramping up fears, such as a desire to fan the flames of Sino-American rivalry or to diminish privacy on the Internet.

But a troubling shift toward censorship, surveillance, and—yes—militarization in cyberspace is very real. Internet filtering is increasingly accepted worldwide, companies have imposed heavy-handed copyright controls, and surveillance in both the public and private sectors is widespread. Meanwhile, there are no international rules of engagement in this domain, and a burgeoning ecosystem of crime and espionage—cultivated by shadowy actors and state intelligence systems that stand to benefit—is ensnaring governments, civil society, and industry *(see "Moore's Outlaws," p. 36)*. All this could soon generate a perfect storm. Individuals might withdraw from cyberspace altogether, gradually eroding the network effects that have benefited us for 20 years.

All armed conflict today invariably includes a cyberspace component: think of the 2006 Israel-Hezbollah war; the 2008 Russian-Georgian war over South Ossetia; the ongoing hostilities in Iraq, Afghanistan, and Somalia; and domestic hostilities in Burma, Tibet, Pakistan, and, most recently, Thailand (among numerous other places). Be it through kinetic strikes on the infrastructure of information and communications technology, missile attacks targeted with the aid of cellular geolocation, espionage that makes fraudulent use of social networks, or privateering that disables key computer networks at critical times, warfare has taken on this dimension because cyberspace is the strategic communications environment in which we all live.

Although invoking fears of an electronic Pearl Harbor may be overheated rhetoric, an arms race in cyberspace creates an environment in which crime, espionage, malware, denial of service, filtering, and surveillance prosper and thrive. In the rush to reject alarmism about cyber war, we should not lose sight of the very real geopolitical conflict that has insinuated itself into this domain and threatens to subvert its architecture. The militarization of cyberspace is not a fantasy but an urgent problem requiring immediate solutions. TR

RONALD DEIBERT IS DIRECTOR OF THE CITIZEN LAB AT THE MUNK SCHOOL OF GLOBAL AFFAIRS AT THE UNIVERSITY OF TORONTO.



GLOBAL HEALTH

Preventing HIV

ROBERT GRANT ARGUES FOR TREATING HIGH-RISK POPULATIONS BEFORE THEY HAVE BEEN EXPOSED.

Preventing HIV transmission is not easy, even though most people know how the virus is spread and are aware that condoms can offer protection *(see "Can AIDS Be Cured?" p. 44)*. An HIV vaccine remains elusive: although a recent trial suggested some success in low-risk populations, the level of protection was not high enough, or certain enough, to justify introducing the vaccine. The first generation of topical microbicides, designed to allow women to protect themselves if their partners refuse to use condoms, was not effective in clinical trials. Male circumcision has been the only clear success: three trials in Africa showed that it partially protected heterosexual men. We still need new protective strategies for women and men who have

NICK REDDYHOFF

USA SCIENCE & ENGINEERING FESTIVAL



USA SCIENCE & ENGINEERING FESTIVAL

A TWO-WEEK CELEBRATION OF SCIENCE: STARTS 10/10/10
Free events, school programs and nationwide contests

EXPO ON THE NATIONAL MALL: OCTOBER 23 & 24, 2010
1500 fun hands-on activities for kids, teens and adults

A FREE EVENT!

USASCIENCEFESTIVAL.ORG

THANKS TO OUR SPONSORS

LOCKEDIUM

FESTIVAL HOST

LOCKHEED MARTIN

LIFETECHIUM

life technologies FOUNDATION

DISCOVERYCIUM

AMERICIUM

POPULAR SCIENCE

SCIENCE ILLUSTRATED

NOBELIUM

Larry and Diane Ecker

EE Times

NewScientist

SCIENTIFIC AMERICAN

Popular Mechanics

ScienceBlogs

EINSTEINIUM

FARRELL FAMILY FOUNDATION

ResMed Foundation

ALEXANDRIA

NORTHROP GRUMMAN

Technology Review

The Epoch Times

KRYPTON

Agilent Technologies

AMGEN

illumina

DOW

Celgene

intel

The Kavli Foundation

WAMU 88.5 FM

C&EN

PLATINUM

VERTEX

K&L GATES

Genentech

PLTW

Sandia National Laboratories

FAMILY

MedImmune

Baxter

Sigma Xi

nvtc

CELESTRON

PALLADIUM

NuVasive Inc.
FEI Company
Case Western Reserve University
Biogen Idec Foundation
LifeStraw®
Microsoft
Draper Laboratory

TITANIUM

Bechtel Corporation
SpaceX
National Radio Astronomy Observatory
SciVee
Research in Motion
SchoolTube
Thirty Meter Telescope Project

sex with men, the people most affected by the pandemic.

Anti-HIV drugs are known to help prevent transmission from infected mothers to infants, which has become rare in parts of the world where the drugs are widely available. Postexposure prophylaxis is recommended by the Centers for Disease Control: a 28-day course of antiretroviral medication after exposure is thought to prevent transmission about 80 percent of the time. But this treatment can't be administered unless people recognize when they have been exposed.

Targeting preventive treatment even before exposure is one solution. Clinical trials being conducted in the United States, Africa, Asia, and Latin America are evaluating whether daily oral use of antiretroviral agents in high-risk groups can help prevent transmission. The drugs selected for evaluation are generally well tolerated, last a long time in the body (allowing for once-a-day dosing and some forgiveness for missed doses), and have shown protection in animal models.

While preëxposure prophylactic treatment seems costly, high-quality generic formulations are widely available at low cost. Another possible objection is that being able to take a pill a day for HIV prevention might cause people to stop using condoms or to have sex with more partners. But I believe it could make prevention services attractive to people who would otherwise deny their risk. Perhaps by serving as a daily reminder of that risk, it could even inspire people to take more steps to protect themselves.

The global spread of HIV will be stopped only if people demand highly effective prevention tools and if those tools become available. History shows that neither will happen easily. Arming people in their struggle against HIV can only help. TR

ROBERT GRANT IS AN INVESTIGATOR AT THE GLADSTONE INSTITUTES AT THE UNIVERSITY OF CALIFORNIA, SAN FRANCISCO.

ENERGY

Photovoltaics Come of Age

SOLAR PANELS ARE CHEAP ENOUGH TO BECOME A MAJOR COMPONENT OF GREEN ENERGY, ARGUES KEN ZWEIBEL.



The United States has supported research into photovoltaics for almost 40 years, recently with a 30 percent investment tax credit. Japan instituted incentives in the 1990s, when photovoltaics cost at least five times as much as residential electricity. In the new millennium, Germany instituted incentives an order of magnitude larger.

Thanks to these efforts, the cost of photovoltaic modules has dropped 40 percent in the last 18 months. Photovoltaic electricity now costs about 15 cents per kilowatt-hour in the best sunlight. That's only twice the cost of wholesale electricity and wind. Costs are expected to continue decreasing, and electricity is worth more during the daytime than at night. That means this technology is finally cheap enough to become a significant element in plans to combat climate change and oil dependence *(see "Solar's Great Leap Forward," p. 52)*.

The advantages of solar panels are clear. They need no fuel or water, and sunlight is nearly limitless. With 100 times the energy potential of wind, sunlight is sufficient to meet all our energy needs. Photovoltaic panels are also unique for their long, low-cost operating life—now 30 to 40 years, someday perhaps 100. And unlike energy sources that require a constant input of fuel, photovoltaic electricity is almost free once its initial capital cost is recovered.

In 2008, when the U.S. Department of Energy drafted a report looking at the potential for "20 percent wind energy by 2030," the plan called for only 5 percent of the country's energy to come from solar power. Soon, the department will publish a new "solar vision" examining the potential for a plan incorporating 10 percent solar photovoltaics, 10 percent solar thermal, and 10 percent wind by the same year. Meanwhile, further DOE work will look at a goal of deriving 80 percent of our energy from renewable sources in 2050. The European Climate Foundation has released a study with McKinsey showing that renewables could produce 100 percent of European electricity by that date. The reports maintain that reaching these targets will have minimal impact on electricity prices.

The ingredients for a fully green solution to climate change and oil dependence are in our grasp. They include electricity from wind and solar photovoltaics; electric vehicles to get us off gasoline; smart grid and transmission technologies to distribute solar and wind power and to balance supply with demand; and domestic natural gas to fill in the gaps. We don't have to turn Earth's crust into a carbon-sequestration experiment, increase our risks with nuclear, or convert arable land to energy farming. We are on track to deploy safe, renewable technologies to stabilize the price of oil and dial down carbon dioxide emissions as much as we want. Confirming photovoltaics' place among these technologies is a big step in the right direction. TR

KEN ZWEIBEL IS DIRECTOR OF THE GW SOLAR INSTITUTE AT GEORGE WASHINGTON UNIVERSITY.

Biometrics: Fingerprints and Beyond

Biometric recognition—the use of biological markers such as fingerprints, iris scans, facial structures or DNA for identification—has begun to move into the mainstream. Governments around the world are rolling out national identity cards that feature biometric identification. The U.S. government has been promoting biometrics-based identity cards for employees at the nation's ports, and has already printed more than 4 million cards for government employees that contain such authentication. And nine of the top ten PC companies offer some system of biometric security on at least one laptop model.

At the present time, fraud and identity theft threaten business and government activities around the world; biometrics-based IDs can provide a level of assurance beyond the typical PIN-code and password security.

Detailing the Biology

Successful biometrics technology demands highly accurate biological images. AuthenTec, based in Melbourne, Florida, developed a sensor that goes beyond the usual practice of employing optics to recognize a fingerprint's peaks and valleys. AuthenTec's sensor employs radio frequencies (RFs) to excite molecules in the living layer of skin where fingerprints are formed. "This RF technology allows us to overcome surface conditions of the skin, where fingerprints can be worn, calloused, dirty, or oily," says AuthenTec president Larry Ciaccia. AuthenTec supplies its biometrics component to consumer electronics manufacturers for use in more than 55 million PCs, cell phones, and other biometrics-enabled products.

It's a continuing challenge to achieve the highest possible resolution and thus the most accurate identification. Cross Match Technology, based in Palm Beach Gardens, designed optical scanners that surpass FBI requirements for fingerprint collection. Its latest scanners can even identify sweat pores that dot the ridges. "More data leads to more accurate matching," observes Michael Oehler, vice president of product management. In addition to single-finger scanners, the company has also developed two-finger, four-finger, and palm scanners, along with systems for face and iris matching.



Source: Cross Match Technologies

Above: The SEEK II combines forensic-quality fingerprint capture, rapid dual-iris scan capability and innovative facial-capture technology.

On the Road

Biometric sensors have typically been large and power hungry; the second generation of biometric devices has been designed for mobility. Law enforcement and military personnel have expressed a need for biometric ID tools that they can carry into the field, so newer readers must be small, handheld, able to operate in challenging weather conditions, and unaffected by collisions with keys, pens, and other objects. What's more, these battery-operated devices must block electrostatic discharge, which has crashed sensor technology in the past.

Orlando-based Zvetco, one of the top sensor manufacturers, uses AuthenTec's technology as a key component of its product. Zvetco engineers developed silicon surfaces to accept fingerprints from dry skin better; protective coatings to guard against weather; and superior electrostatic discharge protection to preclude automatic shutdowns of hand-held devices.

With the use of smart cards on the rise, Zvetco has rolled out a new line of smart-card biometrics readers. Tampa-based Ceelox, meanwhile, has created software that can combine information from different sensor models. For instance, should a company's employees use their own laptops with different biometric sensors, the Ceelox software can integrate the information from these sources and allow all users to access company data.

The Future of ID

Biometric sensors have evolved past simple personal identification: AuthenTec has even developed smart sensors that can be programmed to respond to each individual finger so a PC user can correlate each finger to a different locked application or folder.

Customers in government, industry, and law enforcement keep pushing to increase ID speed. For instance, someone entering the U.S. may eventually have to provide a fingerprint, photo, and iris scan. "Any way we can speed that process up to cut down on queuing time without sacrificing accuracy is important to us," says Oehler.

Security needs continue to grow as increasing numbers of the key activities that support national economies move into digital applications. This is certainly true in the energy sector, where the approaching smart grid will rely on ensuring secure communication among homes, businesses, and utility companies. AuthenTec has moved into this market, and in April the company announced a collaboration with SmartSynch, one of the country's largest providers of smart metering systems, with more than a hundred major utility customers.



Technology Review
PUBLISHED BY MIT

I am the future of technology.

EILEEN STEPHENS
FOUNDER, INNOVISIA

Technology Review reader Eileen Stephens is combining two of today's hottest trends—social networking and clean tech—in her latest startup. She is the founder of InnoVisia, whose mission is to accelerate innovation and startup formation in socially and environmentally responsible business. With a diverse background that includes the successful startup Sage Concepts, a Wharton MBA, and a stint at the White House, Eileen is an entrepreneurial leader to watch. She depends on *Technology Review* to give her "content that is consistently intelligent and subject matter that is relevant to my business," she says. "*TR* has a combination of highly concise snapshots and in-depth analysis of the technology trends that matter."

Thomas J. Gustainis

TECHNOLOGY REVIEW READER PROFILE SERIES

www.technologyreview.com/reader



ROBOTICS

DROP THAT DOUGHNUT!

AUTOM is an automated coach designed to help people stick to a diet and exercise routine. Each day, users check in by using a touch screen to enter information about such things as what they have eaten and how much exercise they have done. The robot provides personalized feedback through synthesized speech and facial expressions. The company claims that people make better progress than they would if they followed the same weight-loss program using a computer or paper log.

Product: Autom **Cost:** Around $500
Availability: End of 2010
Source: www.intuitiveautomata.com
Company: Intuitive Automata

CHRISTOPHER HARTING

SUMMER FUN

TECHNOLOGY FOR THE GREAT OUTDOORS



Stay Cool

THE HANDY COOLER is a personal air conditioner that uses an evaporative cooling system to generate a flow of air as much as about 15 °C below the ambient temperature.

Product: Handy Cooler
Cost: $49.95 **Availability:** Now
Source: www.myhandycooler.com
Company: Standard Merit Research

Stay Powered

USB-ENABLED devices (or two AA batteries) can be recharged with this solar charger, which features thin, lightweight, flexible solar cells.

Product: Be Prepared USB+AA Solar Charger **Cost:** $99.99 **Availability:** Now
Source: www.powerfilmsolar.com
Company: PowerFilm

CHRISTOPHER HARTING



Stay Entertained

THE SOULRA sound system for iPods and iPhones relies on a high-efficiency solar panel to power the speakers and recharge the music player.

Product: Soulra **Cost:** $199 **Availability:** Now **Source:** www.etonsoulra.com **Company:** Eton

Stay Connected

THE PHS300S portable hotspot lets more people bring their laptops on vacation: plug in a cellular modem to connect to Sprint's 3G or 4G network, and the connection can be shared among users over Wi-Fi.

Product: Sprint Personal Hotspot PHS300S **Cost:** $159.99 **Availability:** Now **Source:** shop.sprint.com **Company:** Sprint

SECURITY

Bomb Detector

THE ACRO Explosives Testers are a set of disposable pen-size devices capable of detecting mere micrograms of most common explosives—including peroxide-based explosives, which are typically hard to detect and can be made from household ingredients. The bottom of the cap is touched to a suspicious object or person and then screwed back onto the pen. Plungers at the other end are then depressed in sequence to release reagents. An enzymatic reaction produces a color change if an explosive is present.

Product: Acro Explosives Testers **Cost:** Up to $19 **Availability:** Now **Source:** www.1stdefensegroup.com **Company:** Acro Security Technologies





BIOMEDICAL

ZAPPING ASTHMA

PATIENTS WHO have asthma that is not controlled by drugs may benefit from the U.S. Food and Drug Administration's approval of the Alair medical device. It uses a catheter with an expanding tip made of four electrodes. Inserted in a lung passageway by a medical professional, these electrodes deliver radio-frequency energy, destroying some of the smooth muscle tissue responsible for restricting the flow of air during an asthma attack.

Product: Alair Bronchial Thermoplasty System **Cost:** Not available **Availability:** Now **Source:** www.btforasthma.com **Company:** Asthmatx



LIGHTING

GREEN LIGHT

LIGHT-EMITTING diodes make for bright and long-lasting light sources, but they're not used for general illumination because they don't easily provide bright white light. That may start to change with the 12-watt EnduraLED, a replacement for a 60-watt incandescent bulb. It uses a phosphor film placed a short distance from a high-efficiency array of blue LEDs: the film glows yellow, and the combination yields white light. The LED draws less power than an incandescent and lasts a full 25,000 hours. But the price tag—$60—may leave many people reluctant to change their light bulbs.

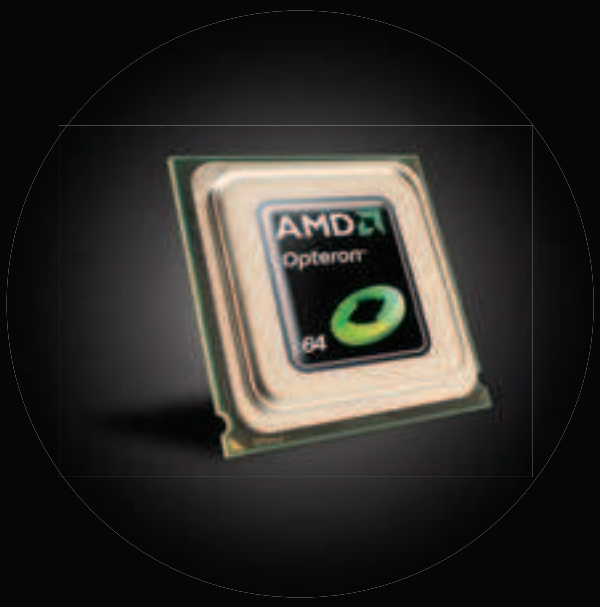
Product: 12-watt EnduraLED **Cost:** Around $60 **Availability:** Late 2010 **Source:** www.lighting.philips.com **Company:** Philips

COURTESY OF ASTHMATX (ASTHMA); CHRISTOPHER HARTING (DETECTOR); PHILIPS (LIGHT)

Cloud Computing with

thunder

with the AMD Opteron™ 4000 Series Platform



The AMD Opteron 4100 Series processor sets the foundation for cloud workloads and affordability for mainstream infrastructure servers with prices starting at $99[1]. An essential component of any cloud computing environment is servers equipped with processors that deliver a balance of performance, I/O capabilities, low energy consumption, and hardware-assisted virtualization. AMD Opteron processors offer these qualities, along with the value needed to drive a cost effective cloud environment.

Learn more at **www.amd.com/cloud/dummies** and download your complimentary copy of *Cloud Computing Clusters For Dummies*, AMD Special Edition.

AMD
The future is fusion

[1] Planned AMD Opteron™ processor Model 4122 1ku pricing at time of introduction

©2010 Advanced Micro Devices, Inc. All rights reserved. AMD, the AMD Arrow logo, Opteron, and combinations thereof are trademarks of Advanced Micro Devices, Inc. 48522A

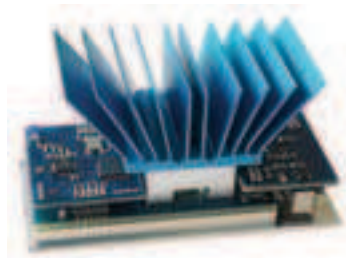
ENERGY

SMARTER CHARGER

MOST CHARGERS continue to consume power even when they are not in use, but the Zero Charger eliminates this waste by turning itself off. Intended primarily for use with cell phones, the Zero uses a USB port to deliver electricity and can sense when no device is attached. If that happens, it stops drawing power from the wall socket.

Product: Zero Charger
Cost: Around $40
Availability: Summer 2010
Source: www.wireless.att.com
Company: AT&T





SENSORS

Harvesting Heat

THE TE-POWER NODE uses any source of thermal energy to drive a wireless transceiver, storing power in a thin-film battery. The Node is a test bed for designers looking to build the next generation of sensor networks, in which the sensors power themselves by harvesting energy from the environment. The battery stores the power that trickles in from sources such as a warm industrial exhaust pipe and then releases the accumulated energy in a pulse powerful enough to operate the radio. A 10 °C difference in temperature produces enough electricity to transmit 13 bytes of information per second.

Product: TE-Power Node **Cost:** $637
Availability: Now **Source:** www.micropelt.com
Companies: Micropelt, STMicroelectronics

TRANSPORTATION

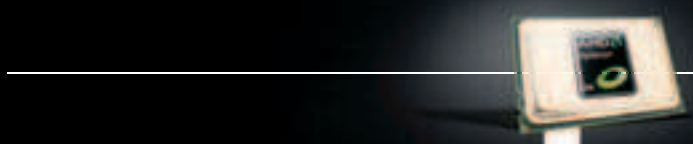
ELECTRIC DELIVERY

THE eSTAR was designed from the chassis up as an electric vehicle for use in cities. Intended to replace fossil-fuel-powered trucks for things like package deliveries, it can haul up to 1,800 kilograms. The truck features a battery pack that can be swapped out in 20 minutes; a fully charged pack will let the eStar travel up to 161 kilometers.

Product: eStar Truck **Cost:** Under $150,000
Availability: Now **Source:** www.estar-ev.com
Company: Navistar

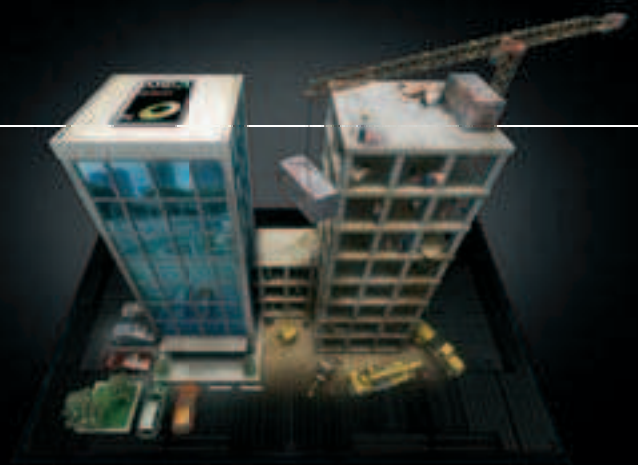


COURTESY OF AT&T (CHARGER); MICROPELT (NODE); NAVISTAR (TRUCK)



Value.

It means more cores for the money, leaving more money for growth.



Unprecedented price per core.[1] The AMD Opteron™ 6000 Series platform.

It's more than a server platform. It's an investment in your future. The AMD Opteron™ 6100 Series processor can give you up to twice the performance of our previous generation.[2] And double the cores at the same price.[3] The AMD Opteron 6000 Series platform delivers as many as 48 total cores in up to a 4-processor configuration at significantly lower prices per core.[1] It gives you the real world performance you need, on a consistent architecture that enables scalability for today and tomorrow. It's the platform to build your business on.

Learn more at amd.com/6000value1

AMD

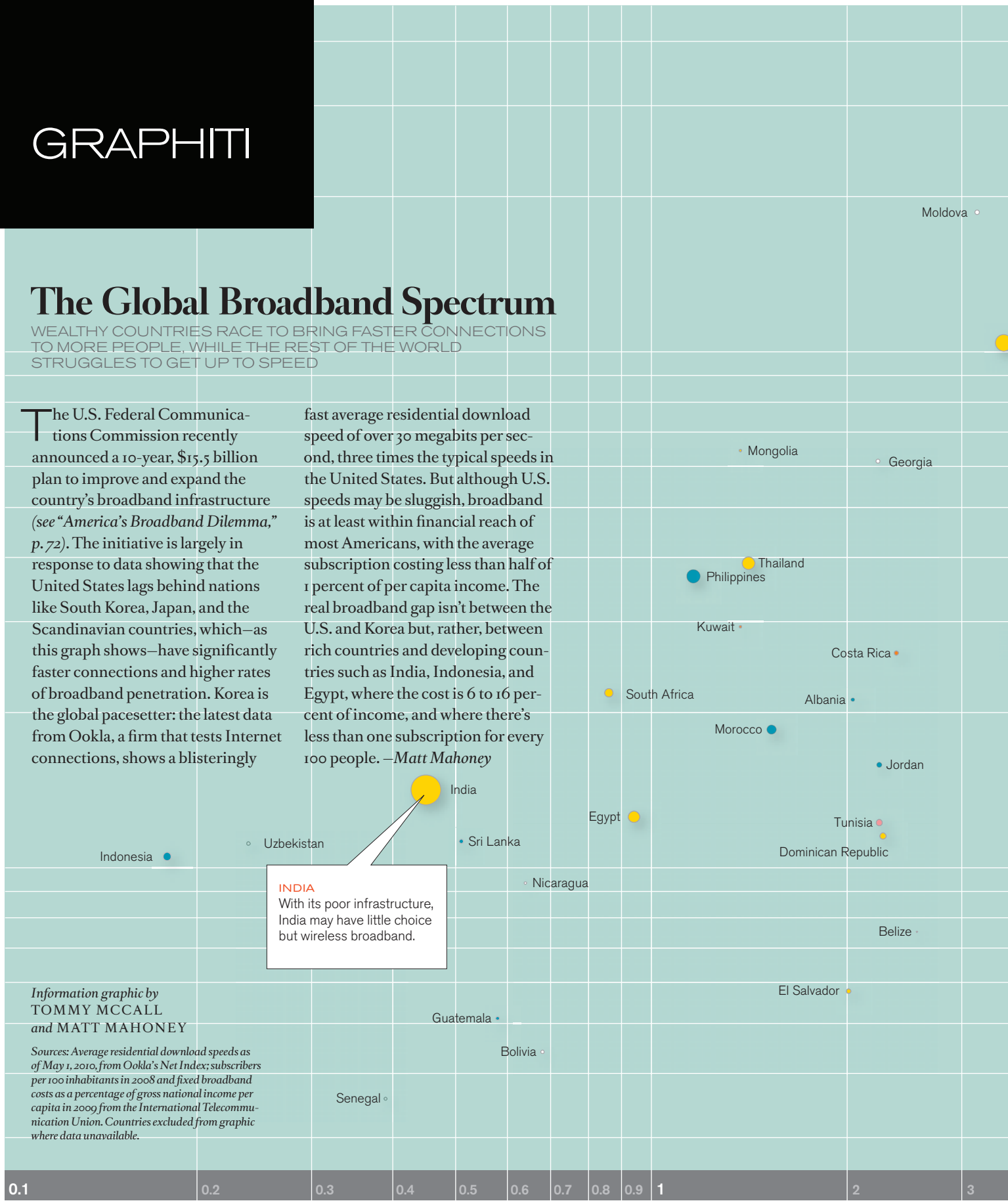
[1]Based on planned 1ku pricing for AMD Opteron™ processor Model 6128 at launch ($266 ÷ 8 cores = $33/core). [2]Internal testing at AMD performance labs as of 2/17/10 showed a 2.13x performance gain (estimate) for 2x AMD Opteron processor Model 6172 ("Magny-Cours") over 2x Six-Core AMD Opteron processor Model 2435 ("Istanbul") running SPECfp®-rate2006. Configuration: "Dinar" reference design, 64GB (16 x 4GB DDR3-1333) memory, 250GB SATA disk drive, SUSE Linux® Enterprise Server 10 SP2 64-bit; Supermicro A+ Server 1021M-UR+B server, 32GB (8 x 4GB DDR2-800) memory, 20GB SATA disk drive, Red Hat Enterprise Linux® Server 5.3 64-bit. [3]Based on comparison of Six-Core AMD Opteron processor Model 2435 (6 cores; $989 suggested 1ku price) vs. AMD Opteron processor Model 6172 (12 cores; $989 planned 1ku price at launch).

© 2010 Advanced Micro Devices, Inc. All rights reserved. AMD, the AMD Arrow logo, AMD Opteron, and combinations thereof, are trademarks of Advanced Micro Devices, Inc. Other names are for informational purposes only and may be trademarks for their respective owners.

The Global Broadband Spectrum

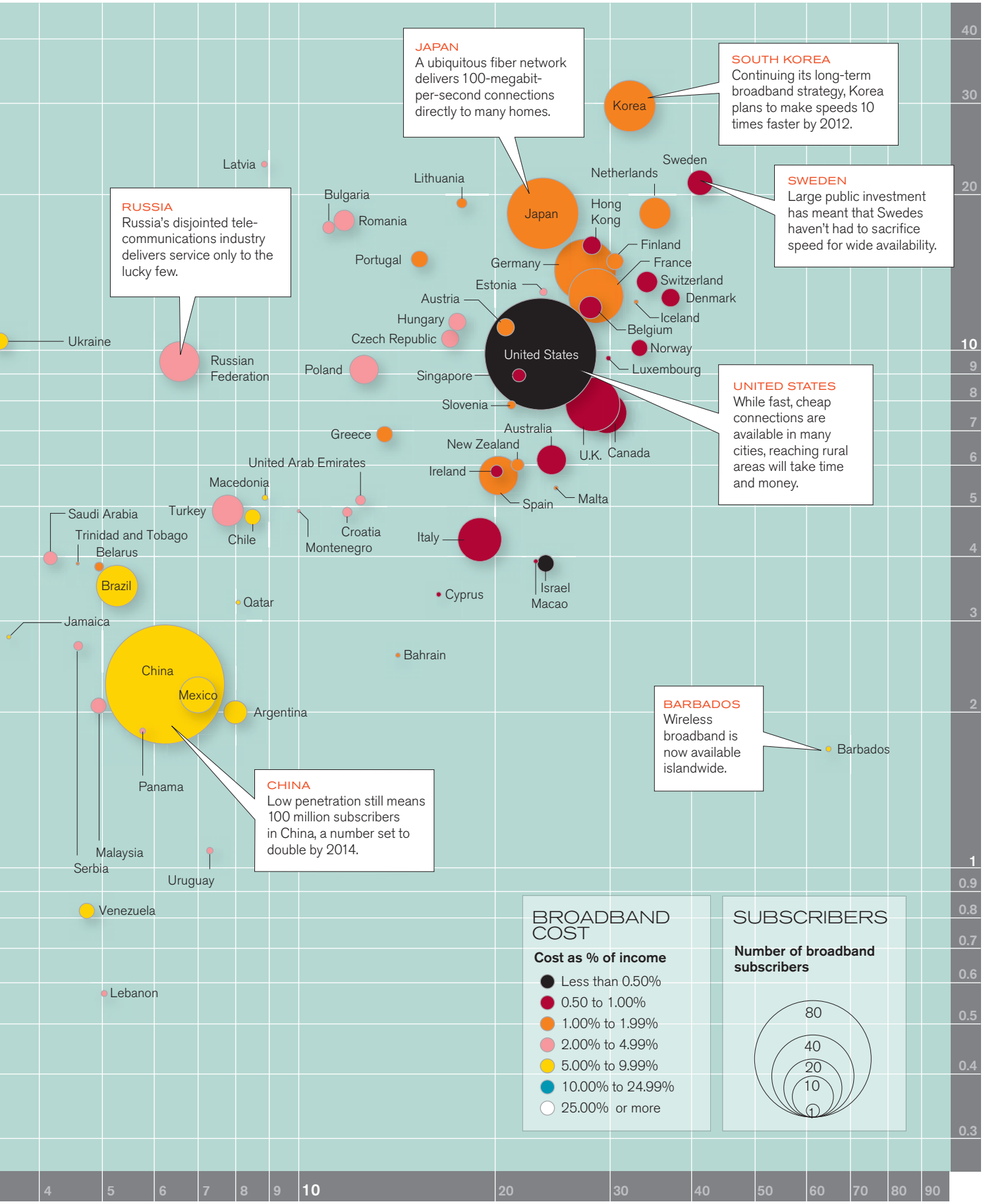
WEALTHY COUNTRIES RACE TO BRING FASTER CONNECTIONS TO MORE PEOPLE, WHILE THE REST OF THE WORLD STRUGGLES TO GET UP TO SPEED

The U.S. Federal Communications Commission recently announced a 10-year, $15.5 billion plan to improve and expand the country's broadband infrastructure *(see "America's Broadband Dilemma," p. 72)*. The initiative is largely in response to data showing that the United States lags behind nations like South Korea, Japan, and the Scandinavian countries, which—as this graph shows—have significantly faster connections and higher rates of broadband penetration. Korea is the global pacesetter: the latest data from Ookla, a firm that tests Internet connections, shows a blisteringly fast average residential download speed of over 30 megabits per second, three times the typical speeds in the United States. But although U.S. speeds may be sluggish, broadband is at least within financial reach of most Americans, with the average subscription costing less than half of 1 percent of per capita income. The real broadband gap isn't between the U.S. and Korea but, rather, between rich countries and developing countries such as India, Indonesia, and Egypt, where the cost is 6 to 16 percent of income, and where there's less than one subscription for every 100 people. *—Matt Mahoney*



Information graphic by
TOMMY MCCALL
and MATT MAHONEY

Sources: Average residential download speeds as of May 1, 2010, from Ookla's Net Index; subscribers per 100 inhabitants in 2008 and fixed broadband costs as a percentage of gross national income per capita in 2009 from the International Telecommunication Union. Countries excluded from graphic where data unavailable.


JAPAN
A ubiquitous fiber network delivers 100-megabit-per-second connections directly to many homes.
SOUTH KOREA
Continuing its long-term broadband strategy, Korea plans to make speeds 10 times faster by 2012.
SWEDEN
Large public investment has meant that Swedes haven't had to sacrifice speed for wide availability.
RUSSIA
Russia's disjointed telecommunications industry delivers service only to the lucky few.
UNITED STATES
While fast, cheap connections are available in many cities, reaching rural areas will take time and money.
BARBADOS
Wireless broadband is now available islandwide.
CHINA
Low penetration still means 100 million subscribers in China, a number set to double by 2014.
Speed (Mb/sec.)
40
30
20
10
9
8
7
6
5
4
3
2
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
4
5
6
7
8
9
10
20
30
40
50
60
70
80
90
Latvia
Lithuania
Bulgaria
Romania
Portugal
Ukraine
Russian Federation
Poland
Greece
Macedonia
Turkey
Chile
United Arab Emirates
Croatia
Montenegro
Saudi Arabia
Trinidad and Tobago
Belarus
Brazil
Qatar
Jamaica
China
Mexico
Argentina
Panama
Malaysia
Serbia
Uruguay
Venezuela
Lebanon
Bahrain
Cyprus
Italy
Slovenia
Singapore
Austria
Hungary
Czech Republic
Estonia
Germany
Japan
Korea
Netherlands
Sweden
Hong Kong
Finland
France
Switzerland
Denmark
Iceland
Belgium
Norway
Luxembourg
United States
Australia
New Zealand
Ireland
Spain
Malta
U.K.
Canada
Israel
Macao
Barbados
BROADBAND COST
Cost as % of income
Less than 0.50%
0.50 to 1.00%
1.00% to 1.99%
2.00% to 4.99%
5.00% to 9.99%
10.00% to 24.99%
25.00% or more
SUBSCRIBERS
Number of broadband subscribers
80
40
20
10
1

Q&A

BUZZ ALDRIN

Apollo astronaut says: forget the moon, let's colonize Mars.

In April, President Obama flew to Kennedy Space Center in Cape Canaveral, FL, to reveal details of his new strategy for NASA and the future of U.S. spaceflight. Sitting next to the president on Air Force One was Buzz Aldrin, who in July 1969 became the second man to walk on the moon. The seating arrangement was appropriate, since both men share a common goal for the nation's space program: reaching Mars by the mid-2030s.

Like Obama, Aldrin opposes the strategy set by President Bush in 2004 to return humans to the lunar surface by 2020. The cornerstone of Bush's plan for NASA was the Constellation program, which included building two new rockets—Ares I to ferry humans into orbit and Ares V to transport heavy cargo—and a manned exploration vehicle called Orion. But the program fell behind schedule and was over budget (*see "The Future of Human Spaceflight," January/February 2010 and at technologyreview.com*). In January, Obama released a new budget proposal that increased NASA's budget by $6 billion over the next five years but terminated the Constellation program.

Technology Review reporter Brittany Sauser recently asked Aldrin about his ideas for the future of U.S. human spaceflight.

TR: Why not go back to the moon?

Aldrin: We explored the moon 40 years ago, and now it should be developed by robots for scientific, commercial, and security reasons. Basically, I don't see a financial return to justify the cost of sending U.S. humans and rockets back to the moon; it's a waste of decades and hundreds of billions of dollars.

What should NASA focus on instead?

The objective should be a permanent presence on Mars by 2035. That's 66 years after Neil Armstrong and I first landed on the moon, and our landing was 66 years after the Wright brothers' first flight. Mars is clearly the best permanent-residence location other than Earth, and we can go there in case somebody or something blows up Earth. We will have a place that ensures the survival of the human race. That means humans who go there commit to staying—one-way tickets will be technically easier and less expensive and get us there sooner.

But that will take years. What should NASA's transition strategy be?

Ares 1 and Ares V should be canceled, and in their place we [should] build an evolutionary shuttle-replacement launch system that could be called something like Ares III [and would transport both people and heavy cargo]. Orion should continue to be developed as an emergency vehicle for the space station, as the president stated. Meanwhile, I also very strongly suggest that instead of retiring the shuttles [in late 2010] and buying rides with the Russians for five, six, or seven years to get to our $100 billion space station, a highly undesirable situation, we stretch out the flights of the five remaining shuttle orbiters to 2015.

The president's plan also relies heavily on the commercial space industry to provide crew and cargo transportation to the space station. Do you think that's a good idea?

Yes, I do. Commercial vehicles will also help fill the gap, so we can develop new launch vehicles and spacecraft for landing on runways for the years beyond 2015 to bring us to the threshold of Mars.

How will we get to Mars by 2035?

We build the ultimate transportation system: a cycling spaceship called the Aldrin Cycler, which I first unveiled in 1985. It cycles between Earth and Mars. Spacecraft can hook up to it, and we could use it to fly by a comet as early as 2018. Then, in 2020, we could travel to a near-Earth object. We would need to build in-flight refueling and communication relays before and during this time, with more visits to asteroids.

In 2025, we land unmanned on Phobos [a moon of Mars] with some elements of habitation. We land people there in 2027 for a year and a half; in 2029 for a year and a half; and in 2031, we land three people who will not come back. In 2031, six people coming from Earth will join the three at Phobos and then continue on to become the first people to land on Mars by 2033 or 2035.

But a consensus on Mars as the goal destination has not been reached. Have you spoken with other influential Apollo astronauts who oppose the termination of Constellation?

I have long been open to discussions with other astronauts, especially the 24 astronauts, 18 of whom are still alive, who reached the moon. But that exclusive group does not have any coherent organization. I am forming a nebulous but much-needed concept for an organization that I call the Unified Strategic Space Enterprise. It would consist of highly respected people who would assist in the development of the national space policy.

It seems like we've been arguing about the future of the U.S. space program for decades now.

We really have only been debating the human spaceflight portions of exploration; where do we send U.S. humans? But there are robotics, the space station, technology developments like in-flight refueling, and all sorts of other things to think about. TR

Photograph by GREGG SEGAL


USA



PHOTO ESSAY

Robot in the OR

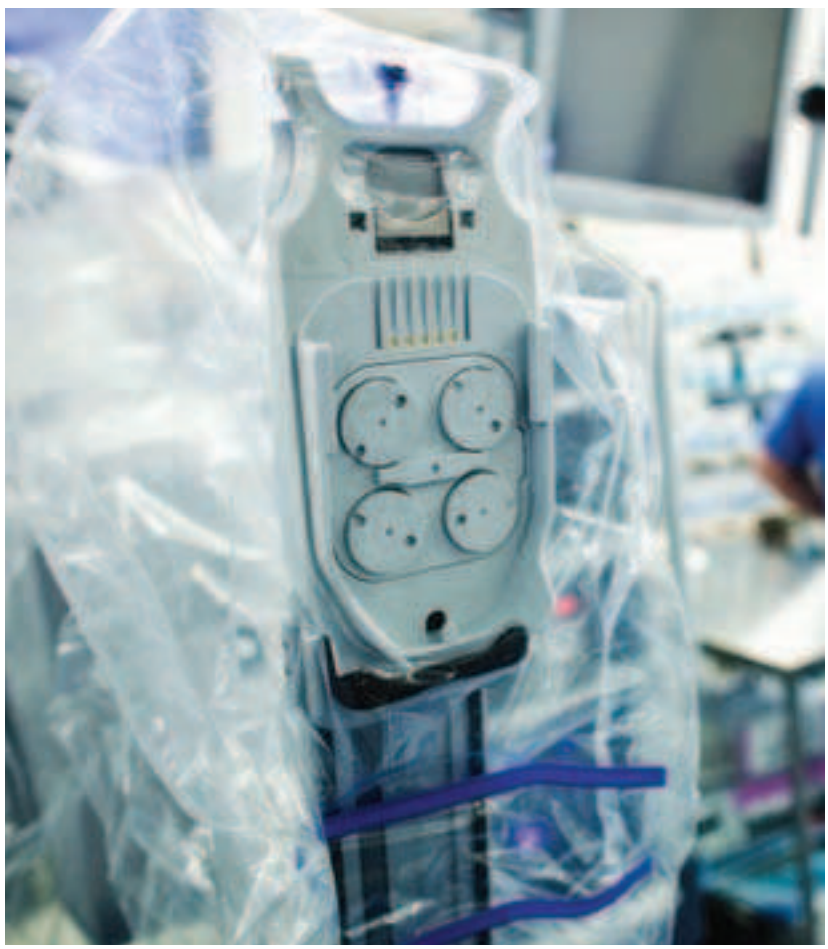
Over the last decade, the da Vinci robot, developed by California-based Intuitive Surgical, has appeared in hundreds of operating rooms around the world. It offers a new approach to laparoscopic procedures, which involve threading surgical tools through small holes in the body rather than making large incisions. Traditional laparoscopy uses tools with limited movement and offers surgeons a flat, 2-D view, but the $2.5 million da Vinci has a sophisticated imaging system and incorporates more flexible tools.

By EMILY SINGER *Photographs by* PORTER GIFFORD



In an operating room at Children's Hospital Boston, surgeons use the robot to repair a three-year-old patient's bladder. The surgeons sit across the room from the patient, manipulating surgical tools through a console.







The robot has three arms (top left), two of which can be tipped with a number of different tools, such as a scalpel, scissors, forceps, or a needle driver for suturing. The third arm holds the imaging endoscope, which lets surgeons see inside the body. Four rotating discs (above left) control the tools' movement, enabling fine precision and multiple degrees of freedom. A hollow port is inserted into the abdomen (bottom photos) so that the small tools can be fed into the patient. Once the tools are attached to the arms, which are covered in plastic to maintain sterility, the large machine is wheeled over to the patient (above right).

Surgeon Hiep Nguyen says the maneuverability of the robot makes it possible to perform laparoscopic procedures on children, whose small body cavities would normally necessitate more conventional surgery.

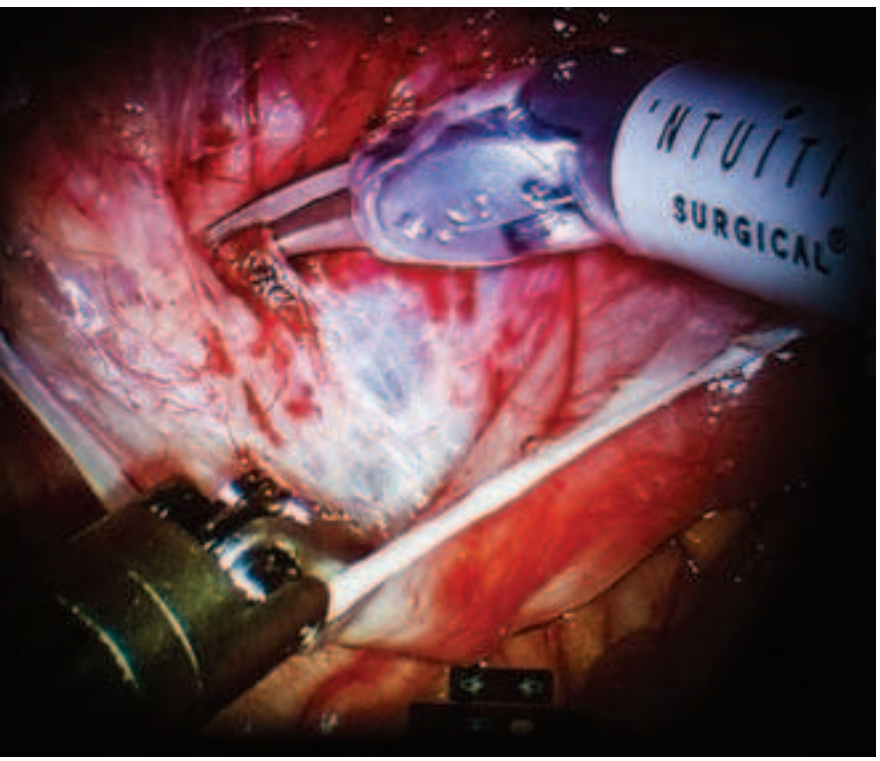






The robot's endoscope holds two small imaging devices that capture two independent images. These are sent to the console, where the surgeon views them as a single stereoscopic image (top left). This view makes it easier for the surgeon to accurately gauge the position of the tools relative to fragile tissue. Nguyen controls the tools by means of two multijointed handles on the console (bottom left). His swift movements (right) resemble those of an expert video gamer. Nguyen jokes that today's gamers will make tomorrow's best surgeons.

In the procedure shown here, called a ureteral reimplant, the muscle of the bladder is wrapped around the ureter to prevent the abnormal flow of urine from the bladder back into the ureter.

















The surgeons' progress can be seen on a number of screens placed around the room (top right) and in the minute movements of the robot's hulking arms (far left). After the procedure, surgeons sew up the small incisions and cover them with bandages (near left).

Nguyen says the system saves his hospital money because patients can go home sooner than they do after conventional open surgeries. However, the benefits of operating with the robot are less clear in procedures, such as prostatectomy, that are routinely performed with traditional laparoscopic tools already. Nguyen, a strong advocate for robotic surgery, would like to see the technology advance faster and become less costly. "The system is very expensive because only one company makes it now," he says. "We need more competition to drive down the price."

Moore's Outlaws

Cyber attacks are increasing exponentially. Here's what recent episodes can teach us about thwarting cyber crime, espionage, and warfare.

By DAVID TALBOT

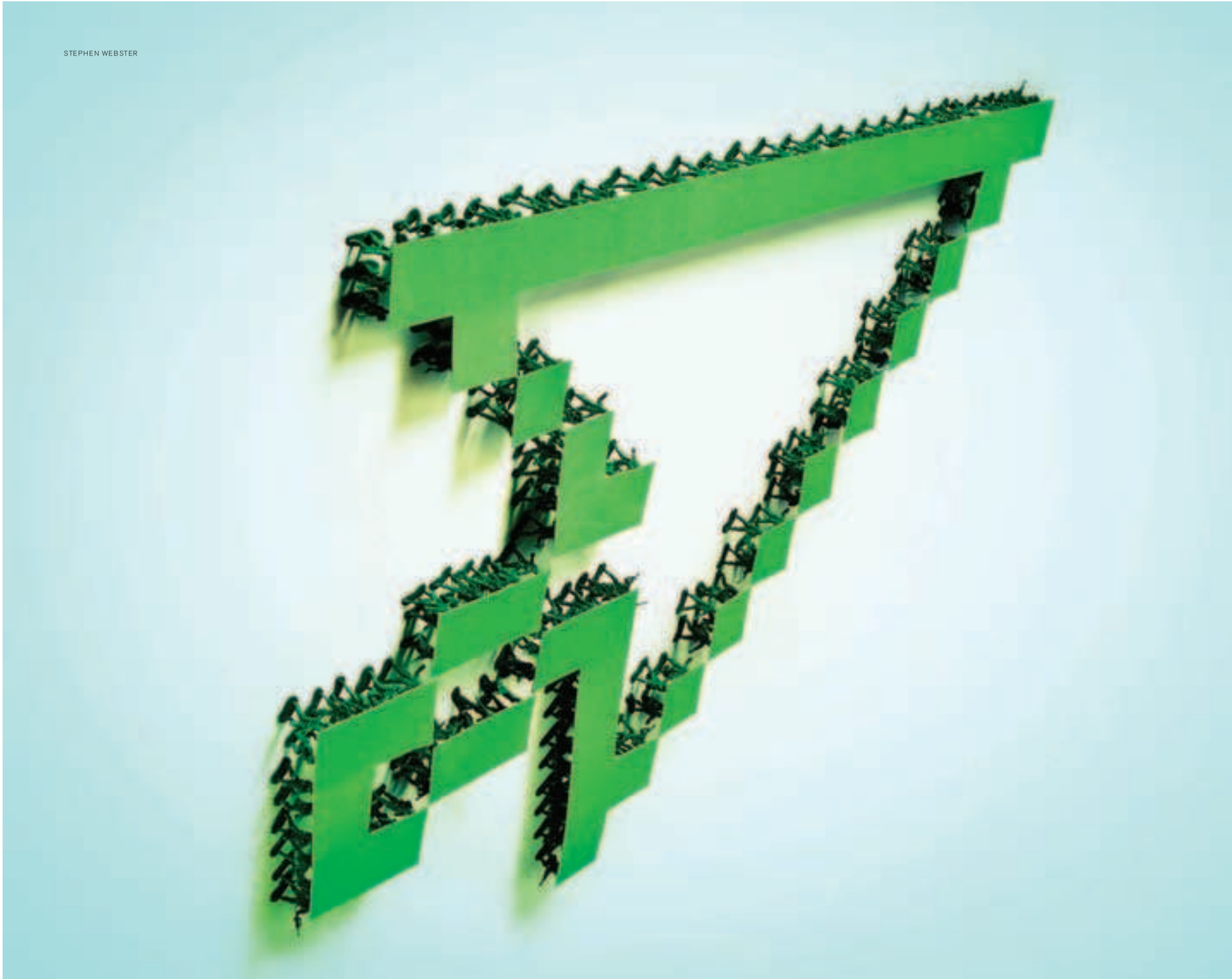
Eugene Kaspersky, CEO of the Russian antivirus company Kaspersky Lab, admits it crossed his mind last year that he might die in a plane crash caused by a cyber attack. Kaspersky is a man of eclectic tastes and boyish humor; when we met in his office on the outskirts of Moscow, he was munching a snack of sweetened, freeze-dried whole baby crabs from Japan, and at one point he showed me a pair of men's undergarments, bought on a Moscow street, that had been stamped "Protected by Kaspersky Anti-Virus." But he grew quite serious when the subject turned to the days leading up to April 1, 2009.

That was the date a virulent computer worm called Conficker was expected to receive an update from its unknown creator—but nobody knew to what end. A tweak to Conficker's code might cause the three million or so machines in its army of enslaved computers, called a botnet, to start attacking the servers of some company or government network, vomit out billions of pieces of spam, or just improve the worm's own ability to propagate. "It's like if you have a one million army of real soldiers. What can you do?" Kaspersky asked rhetorically. "*Anything you want*." He let that sink in for a moment. "We were waiting for April 1—for *something*. I checked my travel schedule to make sure I didn't have any flight. We had no idea about this functionality. Security officials were really nervous." In the end? "Nothing happened. Whew! *Whew!*" Kaspersky cried out. He crossed himself, clasped his hands in a prayerlike pose, and gazed toward the ceiling.

The unknowns about Conficker in the spring of 2009 (the infection remains widespread but, so far, inactive) reflect larger unknowns about just how bad cyber security will get (*see Briefing, p. 59*). The trends aren't promising: tour Kaspersky's labs—or those of any computer security company or research outpost—and you quickly learn that malware is tougher to detect, spam delivery faster, and attacks growing in number and financial impact (*see "The Rise in Global Cyber Threats," p. 43*). Security experts and attackers are locked in a kind of arms race. In Kaspersky's case, his engineers and cryptographers do everything from seeking faster automated virus-detection methods to trolling Russian-language hacker blogs for clues about what's coming.

Ingenious solutions are multiplying, but the attacks are multiplying faster still. And this year's revelations of China-based attacks against corporate and political targets, including Google and the Dalai Lama, suggest that sophisticated electronic espionage is expanding as well. "What we've been seeing, over the last decade or so, is that Moore's Law is working more for the bad guys than the good guys," says Stewart Baker, the former general counsel of the National Security Agency and a former policy chief at the U.S. Department of Homeland Security, referring to the prediction that integrated circuits will double in transistor capacity about every two years. "It's really 'Moore's outlaws' who are winning this fight. Code is more complex, and that means more opportunity to exploit the code. There is more money to be made in exploiting the code, and that means there are more and more sophisticated people looking to exploit vulnerabilities. If you look at things like malware found, or attacks, or the size of the haul people are pulling in, there is an exponential increase."

As these low-grade conflicts continue, the threat of outright cyber war is rising, too. More than 100 nations have developed organizations for conducting cyber espionage, according to the FBI, and at least five nations—the United States, Russia, China, Israel, and France—are developing actual cyber weapons, according to a November 2009 report by the computer security company McAfee. (In May the U.S. Senate confirmed the director of the National Security Agency, General Keith Alexander, as head of the



newly created U.S. Cyber Command.) These arsenals could disable military networks or bring down power grids. And the battle could escalate at the speed of light, not just that of intercontinental ballistic missiles. "Cyber weapons can affect a huge amount of people, as well as nuclear. But there is one big difference between them," says Vladimir Sherstyuk, a member of Russia's National Security Council and director of the Institute for Information Security Issues at Moscow State University. "Cyber weapons are very cheap! Almost free of charge."

That form of battle is still largely speculative and can involve some specialized weapons, whereas the siege of attacks from hackers and malware is a daily reality for individuals and businesses. But the two types of conflict share the same medium, and they could share some of the same approaches. Perhaps most significant, the former becomes easier to wage, and more dangerous, in the murky and chaotic environment created by the latter. "Going after the botnets, going after the corporate espionage stuff, won't remove the threat of disruptive cyber war," says Greg Rattray, a former White House national security official and author of *Strategic War in Cyberspace*. "But a cleaner ecosystem would put a brighter light on cyberwar activity, making it easier to detect and to defend against."

At a basic level, flawed technology is responsible for the whole mess. Many components of our current networks weren't built to be particularly secure (*see "The Internet Is Broken," December 2005/January 2006 and at technologyreview.com*). Report after report from federal agencies, the National Research Council, and think tanks like Rand has made it clear that fixing cyberspace for good will require accelerating research and development to make hardware, software, and networking technologies more secure—and then getting those technologies rapidly in place. The latest call came in a report issued last November by the Department of Homeland Security, which concluded that "the only long-term solution … is to ensure that future generations of these technologies are designed with security built in from the ground up."

But securing cyberspace can't wait for entirely new networks. In the meantime, we must start addressing a host of other systemic problems. Among them: commonsense security practices are often ignored, international coöperation is as spotty as the technology is porous, and Internet providers don't do enough to block malicious traffic. "Hardening targets—and having good laws and good law-enforcement capacity—are the key foundational pieces no matter what other activities we want to try to pursue," Christopher Painter, the White House senior director for cyber security, pointed out at a recent conference. *Technology Review* investigated three recent episodes—an exceptional botnet investigation in Holland, a probe of China-based espionage in India and other nations, and the 2007 Internet attacks on the small Baltic state of Estonia—to glean lessons in how to better police and secure the flawed cyberspace we've got, and prepare for the cyber war we hope will never come.



GRIN AND BEAR IT In the absence of strong international agreements on fighting cyber crime, ad hoc collaboration sometimes gets the job done—as when Eugene Kaspersky, CEO of the Moscow security firm Kaspersky Lab, helped Dutch police shut down a botnet. But such isolated successes are not keeping pace with the exponential rise in attacks.

COURTESY OF KASPERSKY LAB

SHADOW AND GRUM

The Dutchman from the town of Sneek was only 19 years old, but he'd already achieved more than most of us can claim: he'd assumed illicit control of as many as 150,000 computers around the world. The unwitting victims had been rounded up by means of clever messages appearing to come from their contacts on Microsoft's Windows Live Messenger. Those who clicked on a link in the message downloaded a virus; each computer then became a bot. In the summer of 2008, according a U.S. indictment, the man, Nordin Nasiri, decided to sell control of these enslaved machines—a botnet that he called Shadow—for 25,000 euros.

Botnets are among the most serious threats on the Internet. They are the engines behind spam and the fraud and identity theft that spam perpetuates (according to a recent report from the security firm MessageLabs, nearly 130 billion spam messages are dispatched each day, and botnets are responsible for 92 percent of them). They are also responsible for such menaces as denial-of-service attacks, in which gangs of computers flood a corporate or government server with so much traffic that it cannot function. Thousands of large botnets swarm the digital ether, including some that are millions of machines strong. "Botnets are really the root cause and the vehicle for carrying out much of the badness that is going on and affecting everyone," says Christopher Kruegel, a computer scientist and security researcher at the University of California, Santa Barbara.

As things worked out, the Nasiri case was a model for a successful transnational botnet investigation. In the United States, the FBI got a tip about the Dutchman and passed it to the high-tech unit of the Dutch National Police, who arrested him. Then, in an unusual touch, the Dutch investigators sought the help of antivirus companies to craft instructions for erasing the infection from victims' computers and to take over the botnet's command-

and-control system, which operated on servers in the Netherlands. "They wanted to do something novel—to take out the botnet," recalls Roel Schouwenberg, an antivirus researcher at Kaspersky Lab, whom the Dutch police contacted to perform the task. "There was some risk of it getting stolen by other bad guys."

Trouble is, the U.S.-Dutch investigation was an exception. Around the time Shadow was being shut down, another botnet, known as Grum, was gaining strength (*see "Botnet Snapshot," p. 41*). Grum's command-and-control system was hosted by a Ukrainian company called Steephost. In November 2009, Alex Lanstein, a researcher at the U.S. computer security firm FireEye, wrote an earnest e-mail to Steephost's abuse notification address. "Hi Abuse," he began, "I thought you would be interested to know of a criminal network downstream from you." He laid out the facts about Grum and other malicious sites it hosted, but he received no reply. A few days later, however, he noticed the appearance of a kind of botnet fig leaf: the malicious sites' Web addresses now led to phony e-commerce home pages. In March, the computer security firm Symantec said that Grum was responsible for 24 percent of all spam on the Internet, up from 9 percent at the end of 2009.

"With exponential growth in cyber crime, private and public organizations will find cyber penetrations if they look. ... Today, the attacker has the advantage at the architectural levels and is innovating faster than defenders."

Steephost's owners, who could not be reached for comment, had little to worry about in thumbing their noses at the likes of Lanstein. Botnets operate freely across national borders, and law enforcement lags far behind. A treaty that seeks to boost investigative coöperation, the European Convention on Cybercrime, has been signed by 46 countries—mostly in Europe, but including the United States, Canada, South Africa, and Japan. But it has not been signed by China, Russia, or Brazil, which (along with the United States) jockey for leadership as the world's major hosts of cyber attacks. Some signatories, such as Ukraine, are not known for enthusiastic efforts to stop botnets. And attempts to craft a global version have stalled (*see "Global Gridlock on Cyber Crime," Briefing, p. 62*). "Botnets are a serious threat, but we're out of luck until there is international agreement that cyber crime really needs fairly rigorous countermeasures and prosecutions across pretty much all of the Internet-using nations," says Vern Paxson, a computer scientist at the University of California, Berkeley, who studies large-scale Internet attacks.

Given the poor prospects for a global accord, the United States is trying to forge bilateral agreements with some of the worst sources of attacks, including Russia. Russia coöperates on an ad hoc basis in pursuing homegrown cyber criminals—it recently aided in the arrest of several people in Russia who'd allegedly carried out a $10 million online theft from the Bank of Scotland—but stops short of allowing law enforcement from other nations access to its networks. Still, Sherstyuk, the Russian information security czar, told me: "We want to help set the rules in the information sphere. And I bet that there are many things that we can do together."

Many Internet service providers, another potential source of defense, are also making a tepid effort. ISPs have the capacity to identify and quarantine infected machines on their networks, thus containing a source of spam and attacks. But in practice, most ISPs ignore all but those machines so noxious that they prompt other ISPs to retaliate by blocking traffic. It's much cheaper to provide the extra bandwidth than to actually deal with the problem, says Michel van Eeten, a technology policy professor at Holland's Delft University of Technology, who studies botnets. He describes the case of an Australian ISP that was considering technology to automatically cut off infected computers. The ISP soon abandoned the plan when it realized that 40,000 confused and angry customers would be dialing in to customer support lines every month, wondering why they got cut off and how to cleanse their machines. "ISPs typically take care of the bots that trigger countermeasures against the ISP itself," van Eeten says, "but not too many more, because of the cost impact of scaling up such an effort."

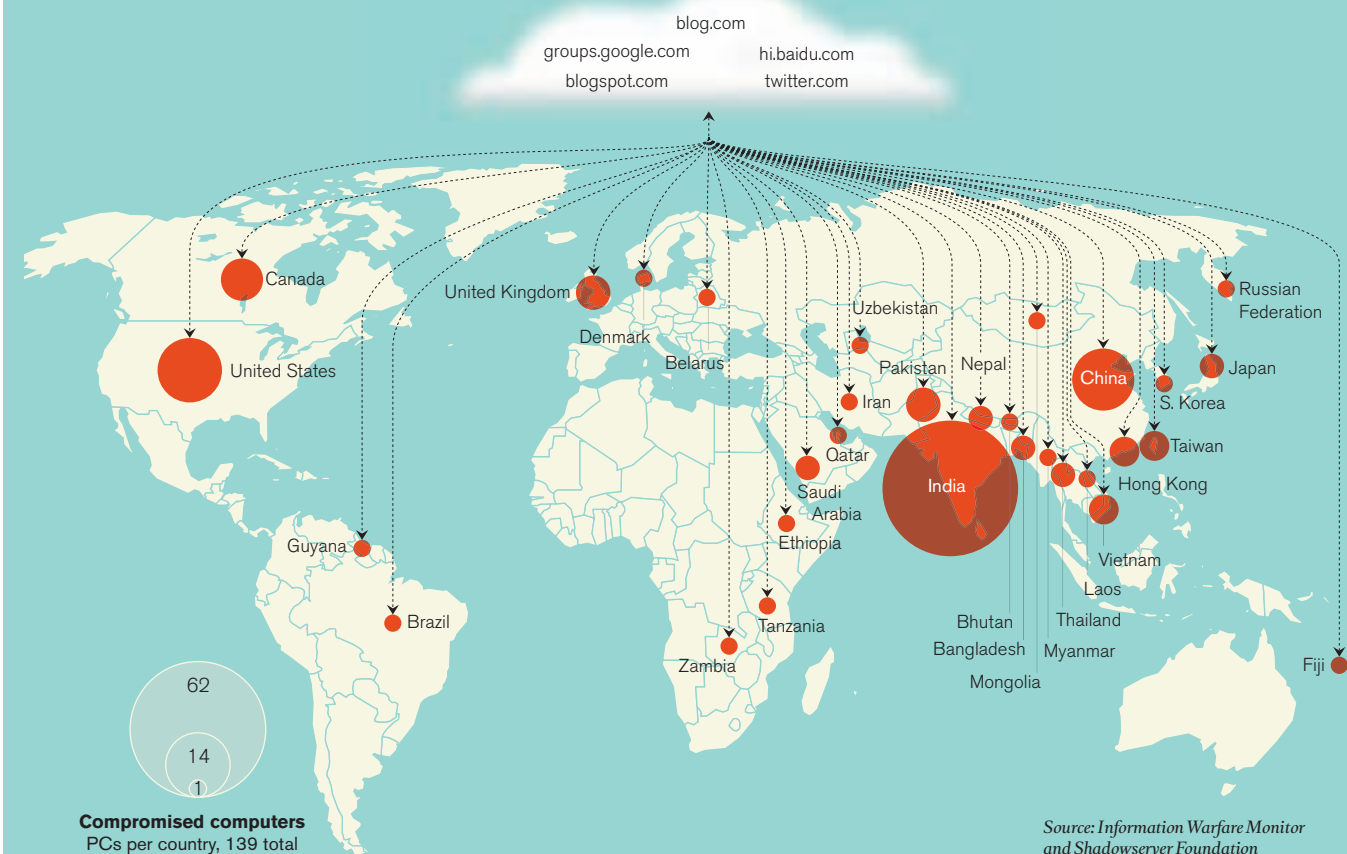
As for the Dutch case, it revealed that even successful investigations are tough to prosecute. Today Nasiri is awaiting trial in Holland on Dutch charges. But a Brazilian man originally charged along with him escaped trial. The U.S. indictment had alleged that the Brazilian orchestrated the receipt of 23,000 euros from a buyer and arranged to receive electronic media from Nasiri containing the bot code. It seemed he'd been caught red-handed. Last year, however, the United States dropped the charges, citing the unavailability of a key witness. The Dutch police say they escorted him to Amsterdam's Schiphol airport and he jetted back to Brazil, a free man.

ESPIONAGE

In 1959 the Tibetan spiritual leader, the Dalai Lama, fled to Dharamsala, a scenic town in the Himalayan foothills of northern India that is still home to Tibet's exiled government. There, a local café called Common Ground also serves as a nongovernmental organization

ESPIONAGE IN THE CLOUD

How China-based hackers exploited Web 2.0 services to run a global spy network



This past spring, researchers uncovered a computer espionage network directed from China by perpetrators who remain unknown. In the map above, circles represent locations of 139 computers known to have been infected with the spyware; they included ones in the National Security Council Secretariat of India, the Office of the Dalai Lama, and the Pakistani embassy in the United States. The infected computers used popular Web 2.0 services (depicted above as a cloud) to check in with attackers' sites, and these sites then sent the machines the addresses of command-and-control servers to which they would connect and send their data. In one case documented by the researchers, 1,500 of the Dalai Lama's letters were sent from Dharamsala, India, to a command-and-control server in Chongqing, China. The researchers suspect that the original infections took root when some victims opened virus-laden Word and PDF documents e-mailed to them. Infected computers were also found in China; some were used by the attackers to test their system.

—David Talbot

that tries to bridge the gap between Chinese and Tibetan cultures. But in 2009, a computer scientist visiting the café discovered a bridge of a different sort: an electronic spy pipeline. The researcher, Greg Walton, noticed that computers in the town's Wi-Fi mesh network, called TennorNet, were "beaconing" to a command-and-control server in Chongqing, China.

The scope of the espionage extended far beyond the café. According to researchers from the Ottawa cyber forensics company SecDev Group (including Walton) and the University of Toronto, victims included agencies of the Indian national security establishment; the compromised data included personal, financial, and business information belonging to Tibetans, Indians, and human-rights figures around the world (*see "Espionage in the Cloud," above*). The discovery came before China-based attacks against Google and other Western companies prompted Google to pull out of China (*see "China's Internet Paradox," May/June 2010 and at technologyreview.com*). "We lack good metrics to figure out how big the espionage problem is, but it seems clear that it's getting a lot worse—and fast," says Paxson. "Google China was a wake-up call, and there's a lot more of it out there."

ALL CHARTS BY TOMMY McCALL

China denies that its government was behind either the Dalai Lama or Google attacks, and the Toronto group says it cannot prove it was. But we can fairly speculate that there is a Chinese market for intelligence about people active in Tibetan circles. Many institutions—corporations, governments, universities—are in a similar position to Tibet's government in exile, in that they hold data worth stealing because it is of value to someone. And the Canadian work shed light on global espionage techniques that, by all accounts, are far more widespread than the China-based attackers' strikes on Tibetan targets. "With exponential growth in cyber crime, private and public organizations will find cyber penetrations if they look," says John Mallery, a computer scientist at MIT's Computer Science and Artificial Intelligence Laboratory. "More or less, organizations are mired in inherently insecure infrastructures and components that were never designed for security and, at best, have been retrofitted with partial security measures. Today, the attacker has the advantage at the architectural levels and is innovating faster than defenders. So what organizations can do is manage their vulnerability by isolating valuable information."

As Mallery suggests, the lesson is that organizations should plan for losses and remain constantly vigilant, because no networked IT infrastructure can be truly safe. Consider that in response to earlier incursions (also detected by the Canadian researchers), the Dalai Lama's staff had installed state-of-the-art firewalls one year before Walton's discovery. But firewalls generally must be programmed to block hostile sites, and the China-based spies used an ever shifting array of benign-seeming intermediaries, including Google Groups, Twitter, and Yahoo Mail. The attackers are believed to have embedded their malware in Microsoft Word and PDF documents sent from seemingly friendly e-mail addresses that had been either spoofed or hacked. If the victim opened the attachment with a vulnerable version of Adobe Reader or Microsoft Office, the spyware took root.

Fortunately, some emerging technologies could provide a solution even in these cases. Cyber espionage often involves sending malicious commands to an infected computer that then sends data back. Detecting the signature of those commands—and then blocking them—is the goal of Santa Barbara's Kruegel, who has developed technology that spots the communication even if the initial infection went undetected. Even though attackers might compromise machines, Kruegel says, if you can identify the commands fast enough, "you can target and shoot them down." He expects to bring the technology to market within one year.

Changes on the political level could also make a difference: right now, no treaty bars what the China-based agents did. While U.N. conventions make strong statements on human rights, for example—and such conventions are frequently invoked to condemn the actions of China and other nations—nothing comparable addresses digital pillaging that victimizes targets in the realms of politics, business, and human rights. "Cyber crime is morphing into cyber espionage because of the absence of restraints at a global level," says Ronald Deibert, who helped lead the espionage research as director of the Citizen Lab, a research outpost at the University of Toronto. "Having a treaty would help hold governments accountable. You can say: 'Here's the treaty, and China, you aren't playing by the rules—but you signed it.'" (*See "Militarizing Cyberspace," Notebooks, p 12.*) Meanwhile, it's safe to assume the worst about the prevalence of cyber espionage. "We need to look at this as one small window into a much wider problem," he says. "We kind of dipped our finger into a pool here."

WHO DID IT?

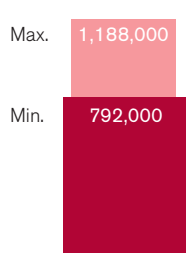
On the morning of April 27, 2007, the Estonian government, over protests from Russia, began moving a bronze statue of a Soviet soldier that had originally been installed in the capital city of Tallinn to commemorate World War II dead. The 300,000 ethnic Russians living in Estonia were furious. Not long after, Internet attacks began. Botnets targeted Estonian newspapers, telecoms, banks, and government sites. The nation's network was besieged for weeks. Russia seemed the obvious culprit: its government had warned that removing the statue would be "disastrous."

If you were watching Estonian network traffic during the attacks, you would have seen bot armies advancing from the United States, Egypt, Peru, and other countries. But closer inspection revealed that many of the bots were taking orders from computers in Russia (and instructions on how to flood Estonian websites with useless "pings" spread in Russia-based online chat rooms). Still, it was impossible to determine whether the Russian government itself was directing the hostile activities. Russia denied responsibility but refused to allow any forensic analysis of its networks.

BOTNET SNAPSHOT

A botnet called Grum is a leading source of spam on the Internet. Here are some of its vital statistics.

Number of bots (infected machines)



Average share of all spam

23.9 percent

Average spam output globally

31.6 billion/day

21.9 million/minute

Spam produced per bot

210,859 /day

146.4 /minute

2.4 /second

Source: MessageLabs Intelligence report, April 2010





BALTIC BATTLE In 2007, following a dispute over Estonia's plans to move a Russian monument (left), riots broke out (above) between Russians and Estonians. Then much of Estonia's Internet was shut down by a series of cyber attacks. The difficulty of attributing those attacks highlights a need for new technologies and expanded international agreements.

In short, there was no easy way to attribute the attack. In a world that countenances the prospect of cyber war, situations like that are among the biggest problems that nations face, but certainly not the only ones. If a network breach aimed at espionage can't readily be distinguished from one that is a prelude to attack, it's hard to know when a counterattack is justified. Neither is there any way to conduct inspections for cyber weapons, measure their potential yield, or certify that they've been destroyed. When the Senate pressed General Alexander, the new head of U.S. Cyber Command, to explain how the United States would deal with these issues, his responses were classified. "The entire phenomenon of cyber war is shrouded in such government secrecy that it makes the Cold War look like a time of openness and transparency," Richard Clarke, the former counterterrorism czar, writes in his new book, *Cyber War: The Next Threat to National Security and What to Do About It*.

But the implications of the attribution problem are clear enough. An attack on one NATO nation obligates other NATO members to join the fight, points out Michael Schmitt, a dean and professor of international law at the George C. Marshall European Center for Security Studies in Germany. Getting it wrong would be a disaster. "This isn't a situation where you can *think* the other side attacked," he says. "You have to *know*. As we learned recently, you need to get the evidence right when you go to war." And in the case of a cyber threat, a government could easily misjudge its source, since Internet addresses can be concealed or faked. "I'm terrified that you attribute to a state wrongly," Schmitt says.

Over the long term, proposed technological fixes could address this problem. Research groups at Georgia Tech, the University of California, San Diego, the University of Washington, and other institutions are working on ways to establish the provenance of data. In an approach being developed by researchers at San Diego and the University of Washington, the identity of the original computer that issued a packet of data would stay attached to that data, in encrypted form. The digital "key" to this identity would be held by a trusted third party—perhaps accessible only by court order. "All the instruments of national power, ranging from diplomatic to military force to economic influence, are pretty worthless if you can't attribute who mounted an attack," says Stefan Savage, a computer scientist at the University of California, San Diego, who is developing the technology. But while the technology can potentially tell you the identity of a machine that waged an attack (or committed a crime), this isn't always helpful if the original source was some public computer. "Being able to attribute activity to a particular machine is a lot different than being able to say 'What was its true source?'" says Berkeley's Vern Paxson. "Even if it went all the way to the terminal end system"—that is, the place of an attack's true origin—"you might have some coffee shop in Shanghai." Paxson warns that in general, approaches to tracking identities in cyberspace carry obvious privacy implications. "The technology to address these sorts of issues—the ability to be able to monitor who is doing what, and track it back—would be very powerful," he says. "But it would also be police-state technology."

With solutions still far off, averting a needless outbreak or escalation of cyber war will have to rely on more conventional intelligence techniques. Surveillance of computer networks can sometimes provide the clues needed to identify and expose a potential attacker, says Bret Michael, a computer scientist at the Naval Postgraduate School in Monterey, CA. So can basic human intelligence networks. If intelligence agencies can pinpoint the source of a threat, they can "shine a light on a malefactor before he attacks or soon after," he says. "Sometimes just being identified is enough to prevent an attack from taking place."

CYBER SUMMIT

On a crisp April morning this year, more than 140 diplomats, policy makers, and computer scientists arrived in the mountain town of Garmisch-Partenkirchen, Germany. Their host was the Russian Interior Ministry. The topic of the conference that brought them there: how to secure the "information sphere," as the Russians put it. But this meant different things to people from different countries. Painter, the White House aide, emphasized fighting cyber

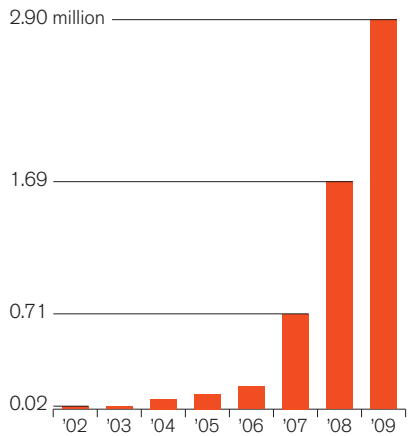
www Watch a video about worsening security and the risk of cyber war: **technologyreview.com/cybersecurity**

DIMITAR DILKOFF/AFP/GETTY IMAGES; RAIGO PAJULA/AFP/GETTY IMAGES

THE RISE IN GLOBAL CYBER THREATS

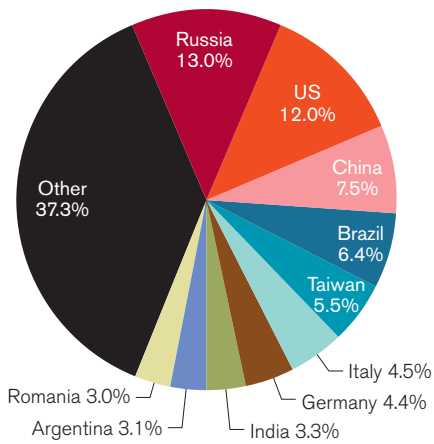
Internet attacks are rising exponentially...

New malicious code signatures



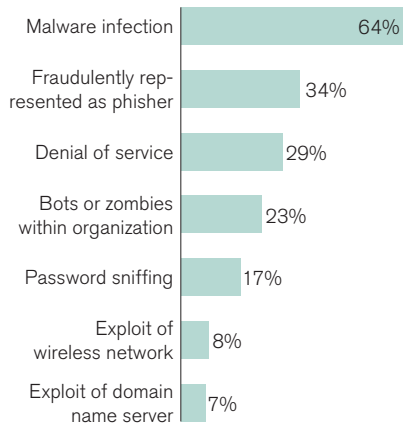
... and are coming from all over the world, requiring a coördinated response.

% of attacks by originating country



The effects of these attacks are felt broadly, as one corporate survey found.

% of organizations affected



Source: Symantec (malicious code); Akamai State of the Internet report for 4th quarter 2009 (global sources); 2009 Computer Security Institute survey of 443 U.S. businesses, government agencies, and other organizations (types of attacks).

crime. Russian speakers—mindful of the suicide bombings that had recently struck the Moscow subway—talked of thwarting terrorist training and organizing online. An Indian researcher talked about network usage by the Mumbai terrorists and described how Indian laws were reformed in response. Representatives of the Internet Corporation for Assigned Names and Numbers (ICANN), the authority responsible for domain names, spoke of the latest security fixes. A small Chinese delegation attended but watched silently.

Then, on the second day, Michael Barrett, the chief information security officer at PayPal, took the podium to remind the attendees of what they had in common: a broken set of technologies. Like other targets, he said, PayPal—which gives Internet users a secure way to send cash in 190 countries and regions—is under siege. "What's becoming clear to us, and indeed any practitioner of information security, is that most of the curves—and we can all dig out these curves, the amount of viruses on the Internet, the number of incursions, and blah blah blah—they all look depressingly similar. They all tend to look logarithmic in scale. They all go up like *that*," he said with a sharp skyward sweep of his hand.

Referring to earlier conversations about improving coöperation and adding security patches, he added: "It's not that those things are bad. But at this point it reminds me slightly of the definition of madness, which is to say, doing the same thing over and over again and expecting a different result. It's our hypothesis that to secure the Internet, we have to think about ecosystem-level safety, and that means rethinking the foundations of the Internet." Just as Barrett was getting warmed up, the Russian organizers cut him off. They were behind schedule and it was time for lunch, but the decision was symbolic of a larger problem. "Essentially, we don't have the technology to address the threats that are delivered by the network infrastructure we've put in place," says John Mallery, the MIT researcher. Several research projects have created test beds for new Internet architectures or prototyped more secure operating systems and hardware architectures, such as chips that store some software in isolated areas. But the Department of Homeland Security report still found "an urgent need" for accelerated research and development on securing cyberspace.

The collective discussion in Garmisch was useful to advance near-term efforts. Changing the behavior of individual computer users and corporations will be crucial; so will tightening law-enforcement ties, installing the latest technological patches, and expanding diplomacy. But switching to new technologies will ultimately be necessary. And that's not likely to happen until we experience a major breakdown or attack. "What we've seen is that arms races often progress in an evolutionary fashion. But now and then, they *jump*," says Paxson. "If there is some cyber attack that messes up a city for a week—or if a big company is brought to its knees—it will be a game changer. I have no way of knowing how to predict that. It's like saying here in the Bay Area, 'Will there be a big earthquake in the next three years?' I really don't know."

His remarks reminded me of Kaspersky's plane-crash fears; collectively, we just can't predict how, and when, things might change. But as Baker put it, "The lesson of 9/11, the lesson of Hurricane Katrina, is that sooner or later, it's going to happen." TR

DAVID TALBOT IS *TECHNOLOGY REVIEW*'S CHIEF CORRESPONDENT.

Can AIDS Be Cured?

Drugs can control HIV, but they exact a steep cost. Now, researchers are pursuing radical new ways to eliminate the infection entirely.

By JON COHEN

In an aging research building at the University of Southern California, a $14.5 million biomedical experiment is under way that until a few years ago would have made many AIDS researchers snicker at its ambition. Mice are the main research subjects (for now), and some 300 of them live in a room the size of a large walk-in closet. Signs plastered to the room's outer door include blaze-orange international biohazard symbols and a blunter warning that says, "This Room Contains: HIV-1 Infected Animals." Yet the hazard is accompanied by an astonishing hope. In some of the infected mice, the virus appears to have declined to such low levels that the animals need no further treatment.

This is a feat that medications have not accomplished in a single human, although daily doses of powerful anti-HIV drugs known as antiretrovirals can now control the virus and stave off AIDS for decades. Every person who stops taking the drugs sees levels of HIV skyrocket within weeks, and immune destruction follows inexorably. The lack of a cure—a way to eliminate HIV from an infected person or render it harmless—remains an intractable and perplexing problem.

"This doesn't look like a multimillion-dollar operation at all, does it?" jokes Paula Cannon, a lead researcher on the project, as she enters the ill-smelling room, which has shelves lined with mice living together in plastic cages that resemble large shoeboxes. As she leads a tour of the cramped space, Cannon wears a face mask, a hairnet, a gown over her clothes, latex gloves, and cloth shoe coverings over her stylish heeled boots. She takes these precautions not to protect herself but to ensure that she won't transmit a dangerous infection to this colony of mice—which is worth somewhere around $100,000.

The experiment costs so much in part because Cannon and her team had to purchase mice bred to have no immune systems of their own; the AIDS virus normally cannot copy itself in mouse cells, making ordinary mice worthless as disease models. Human immune-system stem cells are transplanted into pups bred from these mice when they are two days old, and over the next few months, those cells mature and diversify into a working immune system. Then the mice are infected with HIV, which attacks the immune cells. But before transplanting the original human cells, the researchers introduce an enzyme that interferes with the gene for a protein the virus needs to stage the attack. This modification makes a small percentage of the mature immune cells highly resistant to HIV, and because the virus kills the cells it can infect, the modified cells are the only ones that survive over time. Thus, the HIV soon runs out of targets. If this strategy works, the virus will quickly become harmless and the mice will effectively be cured.

Results from the mouse experiments are encouraging so far, and Cannon hopes they will lay the groundwork to begin human studies soon. "I want to cure AIDS by my 50th birthday," she says; she is now 47. And though she says she is only half serious, her ambition is clear: "I'm looking for a home run."

In the HIV research community, "cure" has long been considered the dirtiest of four-letter words: over the years, various promising approaches have failed, leaving overhyped headlines, crushed hopes, and dispirited scientists in their wake. HIV simply excels at dodging attack, both by mutating and by lying low in a latent, or inactive, form in which it still remains viable. In such a dormant state the virus can survive for decades, completely untouched by the drugs now on the market. Any attempt to flush this latent

Photographs by DANIEL HENNESSY



PRIZED MICE Paula Cannon is using specially bred rodents to test a radical treatment that could lead to an AIDS cure.

virus out of hiding risks doing more harm than good: the treatment itself could be toxic, or it could unwittingly strengthen the infection.

But over the past few years, leading AIDS researchers have begun speaking again of the prospects of a cure. For many, such as Cannon, the goal is a "functional" cure that would allow patients to stop taking antiretroviral drugs without risk of harm from the small amount of HIV left in their bodies. Other, more ambitious investigators want to eradicate the virus totally—what they call a "sterilizing" cure; they are buoyed by an improved understanding of what creates and maintains the reservoirs of latent virus. Either way, the goal is to get HIV-infected people off a lifetime course of drugs.

Douglas Richman, a virologist at the University of California, San Diego, who has cared for HIV-infected people for years, now has patients who have kept the virus completely in check with drugs for up to 17 years. "They're going to outlive me," says Richman, who is 67 years old. "They're not going to die of AIDS. That's wonderful, but do we have to have tens of millions of people on lifetime treatment?"

Such treatment has rising costs, both monetary and medical. In wealthy countries, annual drug expenses run into the thousands of dollars per HIV-infected person. Much cheaper generic versions of the drugs have been given to four million patients in poor countries, but the rich governments footing most of that bill are now cash-strapped and worried about sustaining the charity. And an estimated five and a half million more people urgently need treatment but have no access.

What's more, living with HIV for decades can be medically problematic. Even low levels of the virus can leave patients more susceptible to diseases of aging: heart attacks, malignancies, disorders of the central nervous system. Some of these ailments are side effects of the drugs themselves. People on treatment can have damaging surges of virus, too, when they occasionally stop their drugs or develop resistance to the compounds. "There are five million new infections a year, and three million deaths," says Richman. "So we're just going to have more and more people living with HIV."

Cannon's gene therapy experiment is one of a dozen similar projects in the works that hold the promise of ending patients' dependence on antiretroviral drugs. It's an ambitious dream. But it's no longer as quixotic as it once seemed, and she is approaching her experiment with realistic expectations and the conviction that other researchers' progress will work in concert with her own. "I think in steps," says Cannon. "Will the first person on our treatment be the home run? No. But we may see some benefit. And if you have an imperfect success, it's still a success." Especially when the goal is so grand that it could profoundly alter millions of individual lives—and the course of the AIDS epidemic itself.



SEEKING ANSWERS In experiments that Cannon and her colleagues are conducting, human stem cells are transplanted into mice that have been bred to have no immune systems. Before the transplant, the stem cells are modified so that a small percentage of the immune cells they give rise to will be highly resistant to HIV. The hope is that the virus will run out of immune-cell targets and quickly peter out, effectively curing the animals.

TABOO

Talk of a cure began shortly after the epidemic surfaced in 1981, but for 15 years it was just talk. Even the best HIV treatments did little to hamper the virus. Then, in 1996, researchers reported a remarkable breakthrough using new combinations of antiretrovirals: they could suppress the amount of virus in the blood below the levels that standard tests could detect, allowing immune systems to rebound and people near death to resume normal, healthy lives. Small amounts of the virus could still be detected in these patients by running more sensitive blood tests and analyzing hideaways like lymph nodes or the gut, but the dramatic success of the treatment led prominent AIDS researchers to believe for the first time that the idea of curing HIV was truly realistic.

David Ho, head of the Aaron Diamond AIDS Research Center in New York City, became a media sensation after he spoke at the



In HIV research, "cure" has long been considered the dirtiest of four-letter words: over the years, various approaches have failed, leaving overhyped headlines, crushed hopes, and dispirited scientists in their wake.

international AIDS conference held in Vancouver, British Columbia, in July 1996. Ho had done mathematical calculations showing that if drugs could suppress the virus to this degree, it would take, at most, around three years to eradicate HIV from a patient. His clinical team had an ideal population in which to test the theory: eight patients who had started the powerful drug cocktails shortly after becoming infected, which presumably prevented the virus from ever multiplying to astronomical levels. If all went well for a few more years, these people would stop taking their treatments and, the investigators hoped, never see the virus return.

As much as the headlines celebrated Ho—*Time* magazine named him Man of the Year in 1996—many colleagues were deeply skeptical. "In every field—pancreatic cancer or brain cancer or Alzheimer's—it's okay to say 'I'm working on a cure,' " Ho says. "For HIV/AIDS, it was a taboo."

In May 1997, when Ho and his collaborators published their calculations in *Nature*, they emphasized that surprises might be lurking around the corner. "Although significant progress has been made in the past year in the treatment of HIV-1 infection, it would be wrong to believe that we are close to a cure for AIDS," they wrote. "However, the recent advances in treatment and pathogenesis do warrant a close examination of the feasibility of eradicating HIV-1 from an infected person."

As it turned out, the surprise was lurking in the same issue of *Nature*, which included a report by Robert Siliciano's group at Johns Hopkins University School of Medicine in Baltimore that used a sophisticated assay to identify a reservoir of cells in which HIV infection was latent. Ho's calculations had not included these cells. Siliciano's measurements, however, would show not only that they were detectable in all HIV-infected people, regardless of the virus levels found in their blood, but that they were, by nature, extremely long-lived.

HIV selectively infects and destroys $CD4$s, a type of white blood cell called a T cell that coördinates immune attacks. The cells are so named because of the receptor, $CD4$, on their surfaces—one of two that HIV needs to start the infection process. Once the virus successfully docks on the $CD4$ cells, it unloads its RNA, which is transformed into viral DNA that weaves itself into the human chromosomes in the cell's nucleus. In most cases, the virus makes millions of progeny within a day; they burst out of the infected cell, either killing it directly or marking it for destruction by the immune system. But in some $CD4$ cells, the viral DNA integrated into the chromosomes lies dormant.

The circumstances that cause this to happen are somewhat random, says Eric Verdin, a researcher into the molecular biology of HIV latency who is based at the Gladstone Institute of Immunology and Virology at the University of California, San Francisco. Perhaps the HIV has infected a CD4 cell that is in a "resting" phase of its life cycle, or perhaps the viral DNA has infiltrated an odd part of a chromosome that prevents its genes from operating. "Latency is not a biological property of the virus," says Verdin. "HIV couldn't care less whether it becomes latent." When it does, however, the virus can effectively hide from the immune system—and from antiretroviral drugs. The trouble begins when a resting CD4 cell becomes active after infection or other events somehow activate the virus. Then this latent HIV can launch a new round of viral replication.

In 1999, Siliciano showed that a person on antiretrovirals who has otherwise undetectable viral levels in the blood will still harbor around a million latently infected cells. He calculates that it would take more than 50 years of fully suppressive treatment to clear these reservoirs as the latently infected cells slowly died or the dormant HIV came out of hiding on its own. Indeed, when the patients that Ho's team was studying stopped taking their drugs after their infection had been suppressed for an average of 3.2 years, the virus quickly came back in all cases. Every other research group that tried this experiment had the same dispiriting results. By the turn of the millennium, it was clear that curing an HIV infection would require a new line of attack. Siliciano says, "It's now well accepted that this latent reservoir is going to be a barrier to eradication, and that it's extremely stable and it's never going to decay significantly without specific interventions."

Some scientists argued that HIV returned because the drugs were simply not keeping all of the active virus from copying itself, even in people whose infection was undetectable on standard tests—which can detect the virus if there are only 50 copies in a milliliter of blood. They speculated that a low level of viral replication was sufficient to refill the pool of latently infected cells faster than they could be eliminated. So in several studies these people received extra antiretrovirals, a strategy called intensification. "Absolutely nothing happens," Siliciano says. "The level of virus doesn't budge at all."

Ho and others still believe that the current drugs may be able to fully suppress the virus. But the question has largely become academic, because no intensification effort has yet reduced latent infection in any significant way. Siliciano thinks people should stop expecting more from anti-HIV drugs. He says, "We've reached the theoretical limit."

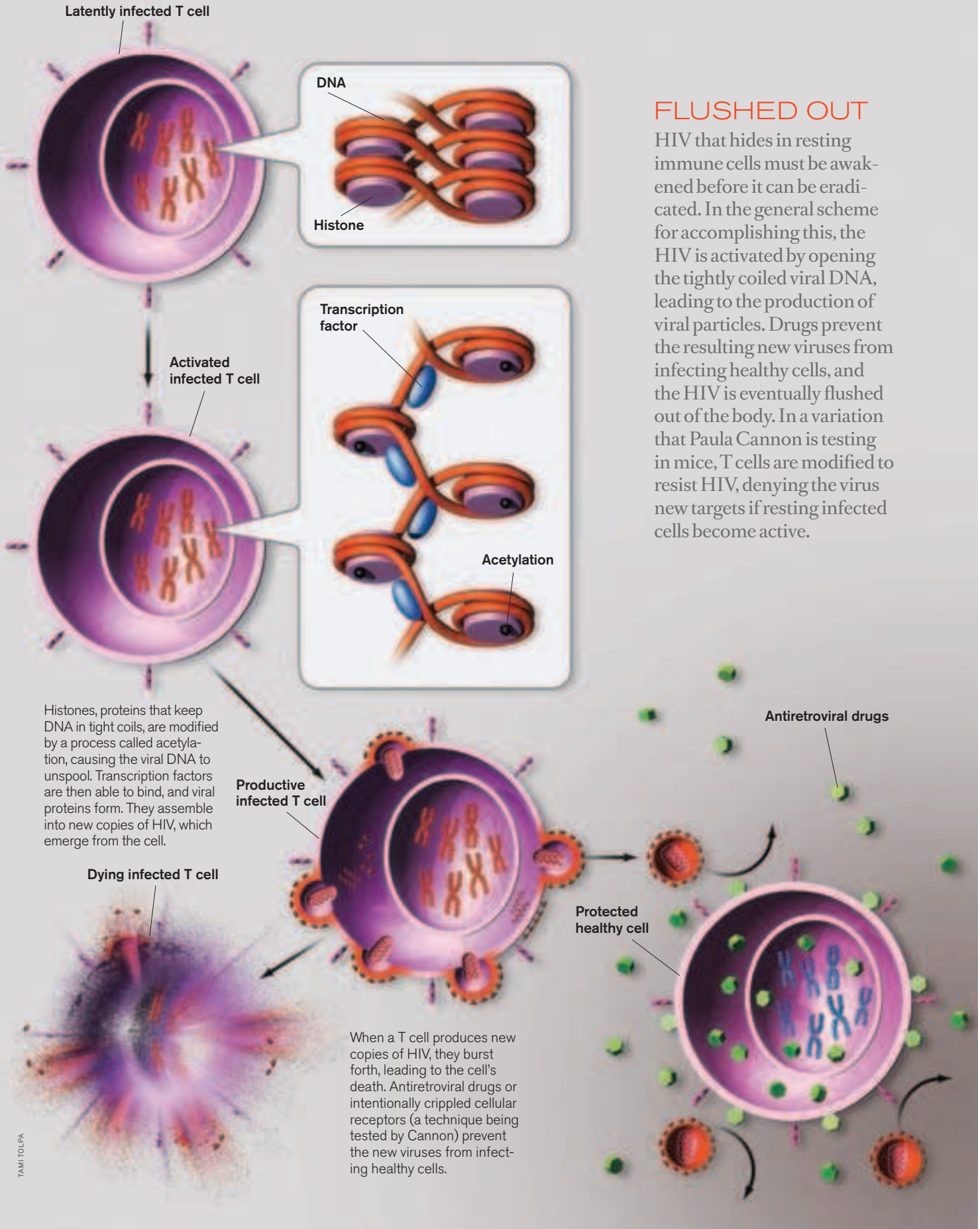
MAGIC FINGERS

In the spring of 2006, Gero Hütter, an oncologist then working at the Charité Medical University in Berlin, saw a 40-year-old patient who had been on anti-HIV drugs for four years. The virus was undetectable in his blood, and his immune system was reasonably intact. But he had another, unrelated problem: acute myeloid leukemia, a blood cancer that threatened his life. Hütter, who now works at the Heidelberg Institute for Transfusion Medicine and Immunology in Mannheim, put the man on repeated rounds of chemotherapy, but after seven months, the leukemia returned. The next option was a stem-cell transplant, which would be preceded by a course of drugs to kill his immune cells—a dangerous procedure called ablation. Although the transplant would come from an immunologically matched donor, some of his own immune cells would probably remain viable, so rejection remained a risk; the physicians would try to reduce it with still other dangerous drugs. One-third of those in the man's condition don't survive the procedure.

Although Hütter was not an HIV specialist, he knew about a mutation found in about 1 percent of people of European descent that makes their CD4 cells highly resistant to HIV. The mutation cripples a second receptor, CCR5, that the virus uses in concert with CD4 to establish an infection. If doctors could find a stem-cell donor who had this CCR5 mutation, Hütter told his patient, the transplant could theoretically enable his body to control any remaining HIV without antiretroviral drugs. "I told him we don't know what will happen, but there might be a chance we'll get rid of HIV," Hütter recalls. "He said, 'I don't care about this—I have no problem with antiretrovirals.' He was scared from his leukemia."

The patient changed his mind, and in February 2007, Hütter and his colleagues performed the transplant with stems cells that had the mutant CCR5. The man then stopped his antiretrovirals. His HIV levels remained undetectable, and the doctors stopped finding evidence of latently infected cells after about two months. A year later, the leukemia recurred; he received ablation with whole-body irradiation and then a second stem-cell transplant. As of today, he remains healthy, and his HIV levels are undetectable by Hütter and his team. Even samples sent to Siliciano's lab and other U.S. facilities that have the most sensitive assays have come up empty. Says Siliciano: "I think he's cured."

The results are tantalizing, but what they mean for most infected people is uncertain. As Siliciano cautions, it could be that destroying his immune cells would have cured the man no matter what replaced them. And although a CCR5 mutation stymies the most common HIV strains, some can use different co-receptors; if they are lurking inside the Berlin patient in latent form, they could one day resurface. Even Hütter says he would like to see a few more years pass with no virus before declaring the patient HIV-free. But there's widespread agreement that he has, at least, been *functionally* cured. "The Berlin patient stunned the whole field, because people didn't expect it would work that well," says Verdin. "It's obviously not replicable to the whole HIV population—the cost,



FLUSHED OUT

HIV that hides in resting immune cells must be awakened before it can be eradicated. In the general scheme for accomplishing this, the HIV is activated by opening the tightly coiled viral DNA, leading to the production of viral particles. Drugs prevent the resulting new viruses from infecting healthy cells, and the HIV is eventually flushed out of the body. In a variation that Paula Cannon is testing in mice, T cells are modified to resist HIV, denying the virus new targets if resting infected cells become active.

the risk, is just incredible. But what it really shows is you can have a functional cure with no other side effects."

Paula Cannon is betting that the immune cells with the CCR5 mutation did cure the Berlin patient. If she could use gene therapy to knock out CCR5 in a person's own stem cells, Cannon would sidestep the thorny problems involved in finding matching donors with the mutation and then combating immune rejection after a transplant. Indeed, her interest in this strategy predates the Berlin transplant, but she says its apparent success has provided further encouragement. "I always thought CCR5 was an obvious target, and the whole thing with the Berlin patient has everyone on the same page," she says. Cannon believes that this case was part of the reason why, last October, the California Institute for Regenerative Medicine awarded her team's proposal more than $14.5 million. "I love the Berlin patient," she says. "I'd like to take him out to dinner."

OTHERS WORKING ON A CURE

FUNCTIONAL CURES

Investigators	Institutions	Project
John Zaia, David DiGiusto, Paula Cannon	City of Hope; University of Southern California; Sangamo	Stem cells modified with zinc finger nucleases to cripple CCR5 receptor
David Baltimore, Pamela Björkman	Caltech	Stem cells with lab-made anti-HIV antibodies
Carl June, Pablo Tebas	University of Pennsylvania; Sangamo	CD4 T cells modified with zinc finger nucleases to cripple CCR5 receptor
Irvin Chen, Geoff Symonds	University of California, Los Angeles; CalImmune	Stem cells with RNA interference to cripple CCR5 receptor

STERILIZING IMMUNITY

Investigators	Institutions	Project
Robert Siliciano, Janice Clements	Johns Hopkins University	Using approved drugs to purge latent virus
Douglas Richman, Daria Hazuda, Ashley Haase	Veterans Medical Research Foundation; Merck; University of Wisconsin	Screening HDAC inhibitors and novel drugs to purge latent virus
David Margolis, Daria Hazuda	University of North Carolina; Merck	Testing HDAC inhibitors and screening novel drugs to purge latent virus
Jerome Zack	University of California, Los Angeles	Screening novel drugs to purge latent virus

In trying to cripple CCR5, Cannon is building on the efforts of many others. Sangamo Biosciences, a biotech company in Richmond, CA, designed an enzyme called a zinc finger nuclease that can specifically target the CCR5 gene and disrupt its function. Working with Sangamo, Carl June, a gene therapy investigator at the University of Pennsylvania, now has a human study under way in which CD4 cells are pulled from HIV-infected people, infected with an adenovirus that carries the zinc finger nuclease, and then reinfused into the patients. But Cannon's work would take things one step further. By targeting the CCR5 gene in the stem cells that give rise to the CD4s, Cannon, who is also working with Sangamo, thinks she ultimately has a better chance of achieving an effective and durable cure.

To test the idea, Cannon's lab transplants human stem cells into one group of mice that serve as controls. A second group of mice receive human stem cells that have been modified with the zinc finger nuclease. The researchers then infect the mice with HIV. Experiments on numerous groups of mice show that the virus initially does equally well in all the animals, but after a few weeks, viral levels nosedive in the treated mice.

The zinc finger nucleases successfully mangle the CCR5 gene in only about 5 percent of the mouse immune cells. But HIV selectively kills the cells whose CCR5 receptors are intact. Thus, Cannon contends, the proportion of cells with a broken CCR5 receptor will increase over a few weeks, until the virus can no longer spread: even if a latently infected cell starts churning out HIV, it has nowhere to go. So the treated mice remain infected, but at such low levels that they suffer no ill effects. "'Cure' doesn't mean you have to eliminate the virus," says Cannon. "You just have to eliminate the consequences of viruses. It's a Herculean task to remove every cell in the body that has HIV in it."

HERCULEAN TASK

Some AIDS researchers still find that Herculean task worth pursuing. To them, the functional cures that Cannon and others are pushing for have merit but do not ultimately solve the problem. After all, an HIV strain that does not need CCR5 may be hiding in the body. Or maybe a latent virus will pop out and somehow mutate in such a way that it does not need CCR5 either. History, of course, is not on the side of those who want to wipe out the virus completely. "It's incredibly heartening to see more people looking at eradication more carefully," says David Margolis, a clinician at the University of North Carolina in Chapel Hill, who has done some of the first drug studies in humans that seek to purge the reservoir of latent HIV. "But it's going to take a lot of hard work by a lot of people for a long time to really make progress. Who knows where the next real advance will come from?"

If current antiretrovirals do indeed completely stop HIV from copying itself, the remaining steps toward eradication will be to

> "'Cure' doesn't mean you have to eliminate the virus," says Cannon. "You just have to eliminate the consequences of viruses. It's a Herculean task to remove every cell in the body that has HIV in it."

identify the location of the latent reservoirs and to flush the virus out of them and into the bloodstream, so the drugs can do their work. Researchers know that one place the latent virus hides is in resting CD4 cells, but Siliciano has published molecular evidence that this cannot be the only reservoir. One recent report from scientists at the University of Michigan suggests that inactive HIV can lurk in bone-marrow stem cells, and the virus could also be in the brain, gut, and lymph nodes. Checking for HIV in any of these tissues is much more difficult than analyzing a blood sample, so it won't be easy to determine how effective a therapy has been at wiping it out.

Regardless of where latent HIV is, the virus must be awakened before drugs can target it. In the late 1990s, David Ho and a few other research groups made a crude attempt to do this. They explored the idea of prodding resting CD4 cells to "activate" and start making copies of themselves; in the process, those latent cells that harbored HIV would transcribe their viral DNA and then die. Ho's group treated one patient with a monoclonal antibody that triggers activation. "He got pretty sick, and we just stopped it," Ho remembers. "It was too scary." A similar attempt almost killed another patient. "For the past decade, it's just been thought of as way too high risk," says Daria Hazuda, who does HIV drug discovery at Merck Research Laboratories.

But safer methods of rousing latently infected cells could now be within reach. "In the last 10 years, there have been enormous new insights into transcriptional control mechanisms of HIV," says Jonathan Karn, who studies HIV gene expression at Case Western Reserve University in Cleveland. "That's been feeding indirectly into understanding latency and how you silence the virus and how it becomes reactivated."

Hazuda is now collaborating with Karn, Margolis, Richman, and other academic researchers to seek new drugs that can flush latent reservoirs. She's scouring Merck's shelves for promising experimental compounds as well as drugs that have already made it to market for other diseases. And she expects more companies to join in soon, partly because testing methods have lately made great strides. Powerful new drug screening assays have been introduced, and novel monkey and mouse models are available. New techniques in genomics and systems biology may also reveal biomarkers that allow researchers to gauge whether potential drugs have had an impact on transcription of the latent virus. "How do you show you've done something meaningful other than take people off drugs and pray the virus doesn't come back?" asks Hazuda. "That isn't a very scientific way to do things."

Even Siliciano, once a skeptic about eradication, now has his lab searching for antilatency drugs. "I've changed because I was really impressed by how easy it was to find compounds that would reverse latency in the test tube," he says.

TESTING HOPE

There is no cure for polio, hepatitis B, measles, chicken pox, influenza, and a long list of other viruses. Though the immune system and drugs can ultimately defeat many viruses, they are notoriously difficult to stop before they cause damage—especially a virus that integrates itself into chromosomes and can lie dormant for years. So it's no surprise that a cure still sounds far-fetched to many experts. Progress, if it occurs, will probably move in fits and starts, especially given the frequent disconnect between what happens in lab experiments and in humans. But the astonishing success of the Berlin transplant suggests that it's possible, and the limitations of the best available drugs show that it's necessary.

If Paula Cannon and collaborators at the City of Hope National Medical Center in Duarte, CA, receive a green light from the U.S. Food and Drug Administration, they plan to begin testing their gene therapy in a small number of HIV-infected adults who, like the Berlin patient, need ablation and a bone-marrow transplant to treat cancer—in this case, a B-cell lymphoma. The subjects' own stem cells will be modified with the zinc finger nucleases that disrupt the gene for the CCR5 receptor. The protocol will be extremely conservative. The patients' stem cells will be harvested four times, and as an insurance policy, the researchers will keep the first batch—the best ones—in reserve, untouched, in case something happens to the genetically engineered cells. Cannon also plans to stitch the zinc finger nuclease into an adenovirus to mimic a technique that has already received approval in Carl June's studies.

Cannon is confident that the human studies will prove the merits of the idea, even if it's only on a modest scale at first. "Our little piece of the puzzle is that we're trying to get zinc finger nucleases to work in stem cells and not do any harm," she says. If her research group can crack open the door, she predicts, colleagues will come rushing in to help find more effective, safer, cheaper ways to functionally cure HIV-infected people of all ages everywhere. "There's nothing like success to galvanize the community," she says. "If we can produce a one-shot treatment that basically means people don't have to take antiretrovirals, it's going to spread like wildfire." TR

JON COHEN, A CORRESPONDENT WITH *SCIENCE*, HAS WRITTEN FOR THE *NEW YORKER*, THE *ATLANTIC MONTHLY*, AND THE *NEW YORK TIMES MAGAZINE*. HE IS THE AUTHOR OF *SHOTS IN THE DARK: THE WAYWARD SEARCH FOR AN AIDS VACCINE*. HIS LATEST BOOK, *ALMOST CHIMPANZEE*, COMES OUT IN SEPTEMBER.

Solar's Great Leap Forward

Suntech CEO Zhengrong Shi made China a powerhouse in photovoltaic technology—and became a billionaire in the process. His next ambition: to make solar power as cheap as conventional electricity.

By KEVIN BULLIS





MADE IN CHINA
Suntech has become a major supplier of solar panels worldwide, including the ones used at this massive eight-megawatt solar farm in Alamosa, CO.

BRIAN BAILEY

To see the future of solar power, take an hour-long train ride inland from Shanghai and then a horn-blaring cab trek through the smog of Wuxi, a fast-growing Chinese city of five million. After winding through an industrial park, you will arrive at the front door of Suntech Power, a company that in the few years since its founding has become the world's largest maker of crystalline-silicon solar panels.

Solar panels cover the entire front face of the sprawling eight-story headquarters. Nearly 2,600 two-meter-long panels form the largest grid-connected solar façade in the world. Together with an array of 1,800 smaller panels on the roof, it can generate a megawatt of power on a sunny day. It's expected to produce over a million kilowatt-hours of electricity in a year—enough for more than 300 people in China.

In 2001, when Suntech was founded, all the solar-panel factories in China operating at full capacity would have taken six months to build enough panels for such a massive array. Suntech's first factory, which opened in 2002, cut that time to a little more than a month. Today, the company can make that many panels in less than one 12-hour shift. By the end of this year, the workers could be done by lunchtime. Suntech's production capacity has increased from 10 megawatts a year in 2002 to well over 1,000 megawatts today. Chinese solar manufacturing as a whole has increased its capacity from two megawatts in 2001 to over 4,000 megawatts.

That rapid growth, fueled by relentless cost cutting, has allowed Chinese manufacturers to overtake those in the United States, Japan, and Germany in less than a decade to become the biggest source of solar panels in the world. Worldwide, Chinese solar panels accounted for about half of total shipments in 2009. And that share is expected to grow this year. Of the 10 largest solar-panel manufacturers, half are based in China. In 2007, U.S. manufacturers supplied 43 percent of the panels for a solar rebate program in California. The rest came almost exclusively from Japan and Germany; only 2 percent came from China. Now Chinese companies supply 42 percent of the panels, and the U.S. share has dropped to 15 percent.

In 2004, it cost about $3.20 per watt, on average, to make silicon solar panels. By now, according to solar-industry analysts at Photon Consulting in Boston, a Chinese manufacturer can make them for as little as $1.28 per watt, while the lowest-cost Western manufacturer will produce comparable technology for about $2.00 per watt. Not only has this cost advantage made Chinese manufacturers dominant in the industry, but it's also helped redefine the prospects for solar power, pushing it closer to what insiders call "grid parity"—the point where it is just as cheap as electricity on the power grid, most of which is generated with fossil fuels. "In about five years' time, we should be able to reach grid parity in at least 30 to 50 percent of the global market," says Zhengrong Shi, Suntech's founder and CEO, speaking from his spacious office looking out over the back of his company's massive solar façade.



FACE OF SOLAR A huge façade of photovoltaic panels (above) greets visitors at Suntech headquarters in Wuxi, China. Suntech's founder and CEO, Zhengrong Shi (right), poses on a deck outside his office, with the façade in the background.

CHEN CAO

Suntech's strategy so far has been to cut the cost per watt by reducing the expense of manufacturing solar panels. But reaching grid parity will also require increasing the efficiency of the panels so that each one produces more watts. Under the leadership of Shi, who was a solar researcher before he became a businessman, the company has developed a new way to make solar panels; multicrystalline modules made last year broke a 15-year-old record for efficiency in converting sunlight to electricity. A few months later, Suntech increased the efficiency mark yet again. And the company's lab has prototypes that promise even better results. If these advances pan out, it could finally clear the way for Shi's dream of affordable solar power.

RICHES AND RAGS

In many ways, Shi reflects the complexity of contemporary China. Though he was born and grew up less than 100 kilometers from his factories in Wuxi, he began his career in Australia, where he lived for a decade and became a citizen before returning to China in 2000 to take advantage of the country's economic boom. "I have to get a visa to work in China," Shi says with a hint of an Australian accent, laughing. Despite his wealth and executive position, he has the casual but confident air of a researcher, wearing a simple sports coat and open-collar striped shirt. But his relaxed look and easygoing Australian mannerisms belie his ambition and his close connections to his native country. Several copies of magazine covers featuring him as the "Sun King" (*Forbes Asia*) and "China's New King of Solar" (*Fortune*) are arranged carefully around his spacious office, amid citations from national academies and other awards. Greeting visitors in the entryway is a huge version of the Ch'an Chu, the Chinese symbol of prosperity—a stone toad gripping a coin the size of a dinner plate in its mouth.

The figure, which is also a symbol of luck, is appropriate. In 2005, when oil prices were volatile and many countries, particularly in Europe, were pushing to cut carbon dioxide emissions, Shi took Suntech public on the New York Stock Exchange. In 2006 he became the seventh-richest man in China, with a net worth of over $1.4 billion, according to *Forbes*. But the man who made Suntech possible very nearly didn't get into solar at all.

Shi's parents, rural farmers left destitute by famines that plagued China in the early 1960s, were forced to give him up for adoption to a close family friend when he was a small child. He excelled at school, ultimately earning a bachelor's degree in optical science and a master's in laser physics. Shi applied to study abroad, as many talented students did in China in the late 1980s. He was approved—not for studies in the United States, as he'd expected, but in Australia. Knowing little about the country, he relied on a suggestion from one of his colleagues that he meet Martin Green, the director of the Photovoltaics Centre of Excellence at the University of New South Wales, who was famous for inventing an approach to



silicon solar cells that achieved record efficiencies. He applied for a paid research position, but Green "immediately turned me down," Shi recalls. Instead, Green persuaded him to study for a PhD. He completed the degree in only two and half years, and in 1995 he started work at Pacific Solar, a startup spun out of Green's lab that was commercializing a new type of thin-film solar cell.

By 2000, Shi was executive director of the startup, but news about the solar industry's growth in Europe and Japan made him impatient. "I saw the opportunity of solar booming," he says. Meanwhile, Pacific Solar's technology was taking too long to bring to market. "Thin-film at that stage was not quite ready yet," Shi says. He also saw an opportunity in China, where costs were low and no one "really understood the technology and the industry." After 10 years abroad, he returned to China and presented a business plan to politicians in charge of the Wuxi New District, a high-tech industrial park about an hour from where he'd grown up. His plan was to make conventional silicon solar panels and do it cheaply. Government officials turned him down, suggesting that even his conservative approach was "one step early," he recalls. Although venture capitalists and large companies offering joint ventures are common now in China, they were rare at the time. So Shi spent the next 10 months making connections and courting politicians while he, his wife, and their two young children lived off his savings. "The real challenge was convincing local government officials that I could succeed in the solar business and not just in the solar laboratory," he says. Eventually they offered him $6 million, collected from local state-run businesses, to start Suntech.

Shi kept an eye out for every opportunity to cut costs. He bought used equipment. He helped a Japanese company design a new machine in exchange for a discount. And where he could, he found ways to replace machines with cheaper labor.

The manufacturing methods Shi used to get the company off the ground can still be seen in the factory, which is accessible through doors at the back of the headquarters building. Workers, rather than the expensive robots used in solar factories in Japan and the West, transfer eggshell-thin silicon wafers one by one onto racks that can withstand blazing furnaces where temperatures reach 1,000 °C. The operation could be automated, but human labor costs less and can reduce breakage rates. Machines are used where they're worth it: at another station, one tests the power output of finished cells with a flash of light before robotic arms place them into bins according to performance. A human crew sorts those cells further, identifying fine gradations in the deep blue color. (All this sorting is done to ensure the consistency of the cells that go into a panel.) In another building, workers weld solar cells together into strips, then align them by eye on a light box to form the rows and columns of cells that make up a complete solar panel. To finish the panels, pairs of workers glue the frames together by hand and clean them off with a rag.

ON DEMAND

When Shi started Suntech in 2001, his timing couldn't have been better. Solar manufacturing in China was almost nonexistent, so he had little domestic competition. At the same time, the market worldwide was starting to grow. Price incentives for solar power that the German parliament authorized in 2000 were just going into effect *(see "The German Experiment," p. 76)*; after those subsidies were increased in 2004, Germany became the world's largest market for solar panels and Suntech's biggest source of revenue.

As other governments introduced their own incentives for installing renewable sources of energy, demand soared, and build-

ers began taking a chance on the cheap solar panels coming out of China. "In 2005 and 2006, I couldn't get solar panels," says Barry Cinnamon, CEO of Akeena Solar, a solar installer and one of Suntech's first customers in California. "Demand was way bigger than supply. Any company, anywhere in the world, that could make a piece of glass with wires on it that generated electricity when the sun hit it could sell as many as they wanted." Not only could Suntech meet his demand, but it was willing to accommodate Akeena's requests. "What was interesting about Suntech was they were willing to build a specially designed solar panel for us," he says. "Nobody else would do it."

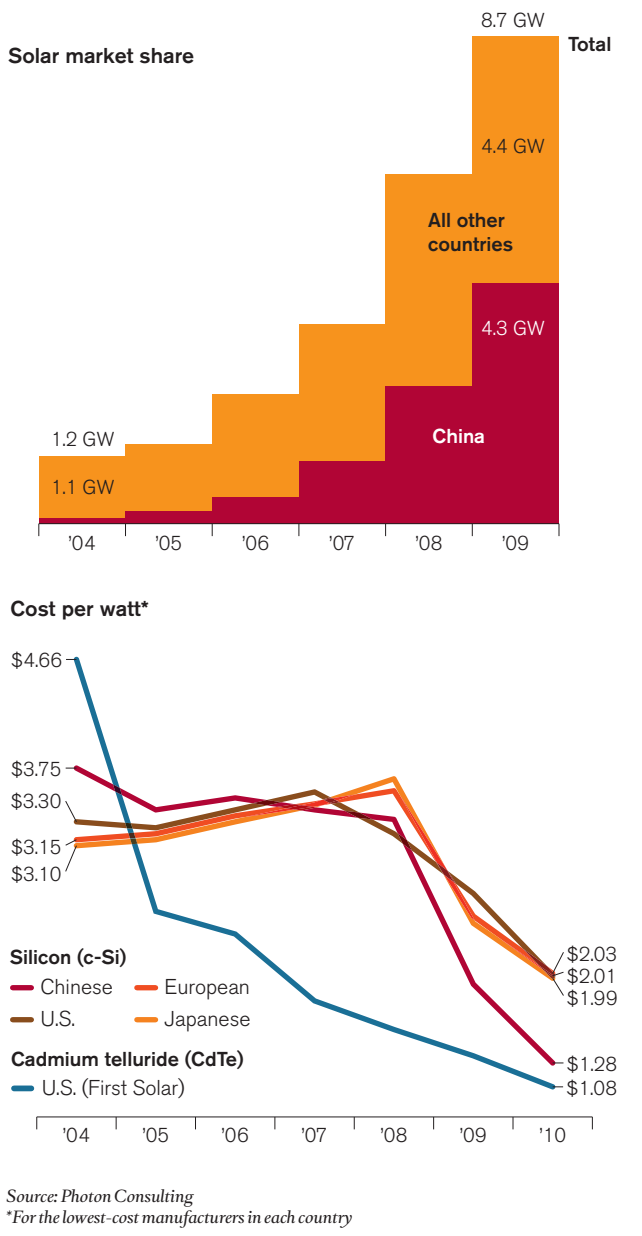
In the years after Shi founded Suntech, the total number of watts produced by the solar industry doubled roughly every two years. Suntech stayed ahead of the curve, doubling its own production on average every year until 2009, when the recession slowed things down. This year its production is likely to grow by 100 percent yet again; the company will employ 12,000 workers. The government recently made Suntech eligible for $7.3 billion in loans through the Chinese Development Bank to fund even more expansion.

Meanwhile, hundreds of other solar companies have been founded in China, and several have become major suppliers worldwide. Yingli Green Energy, based near Beijing, has an even bigger share of the California market than Suntech, though it produces fewer panels overall. It also has even lower costs. Others, such as JA Solar, Trina Solar, and China Sunergy, are rapidly gaining brand recognition worldwide. Much of the industry can be traced back to Green and his lab in New South Wales; former students of his are key leaders in companies that together produce 60 percent of the solar panels made in China. But if Green supplied much of the technical training, he credits Shi with the business savvy to help create the nation's booming industry. "Former students have had a big impact in China," he says. But, he adds, "I would give all the credit to Zhengrong Shi for blazing the trail the others have followed."

GREEN TRICKS

When he founded Suntech, Shi knew that it was possible to manufacture solar cells nearly twice as powerful as the ones that rolled off the line of his first factory. Green had been making them for years in his lab. If you alter the electronic properties of the very highest-grade silicon wafers in precise patterns and then trace extremely fine electrical contacts on their front and back surfaces to extract electronic current, the resulting cells capture much more of that current than conventional cells do. The only problem is that Green's methods rely on advanced and expensive processing technology borrowed from the semiconductor industry. The cells cost about 100 times as much to make as conventional solar cells like the ones Suntech has been producing so far.

CHINA'S PROGRESS



Source: Photon Consulting
**For the lowest-cost manufacturers in each country*

The University of New South Wales had been trying unsuccessfully to commercialize the technology for 20 years, but Shi was determined to find a way. The key was to identify low-cost methods of achieving the same effects with readily available, commercial-grade silicon. Pointing to its 45 patents and 65 pending patents, Suntech claims it has now succeeded, but it's secretive about the details. Only three employees have seen the whole pro-

cess of making its new products. "We know that anyone who has seen the entire line will be targeted very, very enthusiastically by other companies," says Stuart Wenham, Suntech's chief technology officer. Wenham, a colleague of Green's at New South Wales and of Shi's at Pacific Solar, was brought in to Suntech in 2005 to produce the advanced cells. "Dr. Shi was so determined to keep all of this confidential that he bought his own equipment company to make the equipment for this technology," he says.

The process involves replacing a key step in making conventional solar cells: screen printing. To extract electrical current from a cell, manufacturers print lines of silver paste on its front surface. The closer together these electron-conducting lines are, the more efficiently they'll collect charge from the silicon. If too much of the cell's surface is shaded by the lines, however, the cell can't absorb enough light. The thinner the lines are, the closer they can get without causing this problem, but the printing process can't make them thinner than about 120 micrometers.

The Suntech researchers developed a way to chemically treat the silicon wafer in narrow bands. These treated areas attract silver, which forms metal lines just 20 micrometers wide. In addition to resulting in thinner lines, the process makes it possible to save material costs by using wafers of silicon so thin that screen-printing equipment might break them as it stamped the lines on their surface. It also replaces a treatment used in conventional manufacturing that reduces the cells' efficiency by damaging the surface of the silicon. The best modules made with the new technology convert about 18 percent of the energy in light into electricity—as opposed to 13 percent for the company's original solar panels. Next year Suntech intends to roll out a newer version of the technology, which preliminary tests suggest will improve efficiency by another one or two percentage points. The improvement might seem modest, but increased efficiency has a big impact on the cost of the resulting electricity. As a rule of thumb, a percentage-point improvement in efficiency can cut costs by over 6 percent.

Suntech is also funding collaborations with universities, including New South Wales and Swinburne University of Technology in Melbourne, to develop solar cells that get around a fundamental limitation of today's photovoltaics: they can't absorb all the wavelengths in sunlight, and they can't convert all the energy in many of those wavelengths into electronic charge. One key investment is in plasmonics, which makes use of the fact that metal particles deposited on a cell's surface can guide light energy so that it bounces back and forth within the cell instead of being reflected back out. Exploiting this effect could enable researchers to reduce the amount of active semiconductor material in a solar cell by orders of magnitude, or even to make cells out of materials far cheaper than purified, crystalline silicon *(see "Light-Trapping Photovoltaics," May/June 2010 and at technologyreview.com)*. "Those concepts will probably not find their way into commercial products in the next 10 to 20 years," Wenham says. "But they will eventually."

www Listen to the CTO of Suntech explain the company's advanced solar technology: **technologyreview.com/suntech**

ON THE VERGE

In spite of the rapid growth of Suntech and the solar industry worldwide, solar power still contributes a vanishingly small portion of the total electricity produced each year. In the United States, it's slightly above 0.1 percent. "It's a rounding error," says Nathaniel Bullard, an analyst for Bloomberg New Energy Finance.

It's hard to project the course of the still tiny industry. For one thing, all predictions of when solar power might reach grid parity are rife with uncertainties, Bullard says. To take just one example, consider that today the solar panels themselves account for less than half the total cost of the technology. The costs of installation, additional equipment such as inverters, sales and marketing by installers, and, crucially, financing will also need to come down. What's more, when it comes to grid parity, the price that photovoltaics manufacturers charge for their products is actually more significant than the money it costs to make them—and that will depend on the market. If demand for photovoltaics remains high, in part because government incentives in Germany and elsewhere prop it up, then solar panels could remain expensive enough to keep the price of solar energy well above that of electricity from the grid.

It's also not yet clear what technology is best suited for widespread use of solar power. Ten years from now, the solar panels most people buy might not even be made of silicon. Switching would be hard for Suntech. While it has the expertise to change direction, its low manufacturing costs depend on investments in equipment and agreements with silicon suppliers. Meanwhile, rival companies have a head start on the technologies that use other materials. First Solar, based in Tempe, AZ, makes thin-film solar cells made of cadmium and tellurium for even less per watt than the Chinese companies making silicon cells. Admittedly, First Solar's technology converts only about 11 percent of sunlight into electricity; that relatively low efficiency translates into higher installation costs and limits the applications it's good for. Still, thin-film solar is accounting for a steadily greater share of the overall market, from 3 percent in 2003 to more than 15 percent today.

Yet for all this uncertainty, Shi remains convinced that silicon-based solar power is on the verge of becoming competitive without government subsidies. The idea that solar energy will have to wait for a breakthrough to reach grid parity is "crap," he says. He adds: "We're not talking about rocket science. We're talking basic engineering." TR

KEVIN BULLIS IS *TECHNOLOGY REVIEW*'S ENERGY EDITOR.

WHAT'S *the* BUSINESS PROBLEM?

PROTECTION
PROTECTION
THE ROAD

TOO LITTLE PROTECTION ON THE ROAD

the QWEST SOLUTION: No matter where your workers go, risks to your network will follow. Qwest's suite of security solutions can help make sure your critical information is accessible to those who need it on the road, while protecting it from those who don't. So your business can safely stay on the go. **Solve more problems at qwestsolutions.com.**

Qwest BUSINESS

Copyright © 2010 Qwest. All Rights Reserved.

60 TECHNOLOGY OVERVIEW
61 INDUSTRY CHALLENGES
62 CASE STUDY
62 POLICY
63 RESEARCH TO WATCH
64 THE BIG PICTURE
65 OVER THE HORIZON
66 MARKETWATCH
67 COMPANIES TO WATCH

BRIEFING
COMPUTER SECURITY

Large-scale cyber attacks drive new defenses



LARS LINDQVIST/KONTINENT/REDUX

Hackers gather at Dreamhack, the largest computer gathering in the world, held twice a year in Sweden.

Over the past few years, computer attacks, once largely a nuisance issue, have become a threat to national security. Organized criminals have taken advantage of the shift toward online banking and commerce to compromise the financial identity of millions. Even worse, it's now possible for hackers to cripple government websites during a conflict, or for governments to spy on businesses. Some people even fear that cyber terrorists could use the Internet to damage critical infrastructure such as power stations *(see "Moore's Outlaws," p. 36)*. Concrete numbers on the economic impact of security failures are hard to come by, but the FBI says that losses from cyber crimes in the United States jumped 112 percent from 2008 to 2009.

Cyber attackers exploit fundamental weaknesses in our computer systems *(see "The Attacker's Advantage," p. 60)*. And the threat only grows as more and more businesses around the world become dependent on the Internet, and as more critical infrastructure goes online. To prevent a disaster, experts are working on new defensive technologies, and organizations are even tightening up internal security to protect themselves from malicious insiders. But given that the attackers and their victims are often in different countries, international coöperation will be crucial to improving security, and the necessary agreements have proved hard to reach *(see "Global Gridlock on Cyber Crime," p. 62)*. *–Stephen Cass*



Last year, Google was the victim of cyber attacks originating in China that stole software and targeted human-rights activists.

TECHNOLOGY OVERVIEW

The Attacker's Advantage

No one is exempt from cyber attack. In January, Google admitted that its systems had been breached and intellectual property stolen; in April, it was revealed that hackers had stolen military documents from India's government; and stories about the online theft of credit-card numbers and other personal information are constantly streaming in. Why are computer systems so vulnerable?

It comes down to how most software is designed, says Andy Ellis, senior director of information security and chief security architect for Akamai, an Internet infrastructure company based in Cambridge, MA. Companies build systems that often have more functions than users really need. Security is often an afterthought. But if any one of those functions has a mistake in design or implementation, that's all it takes to give attackers the opening they need.

One widely used attack takes advantage of a vulnerability known as a buffer overflow. When information sent to a program over the network exceeds the space that the programmer has set aside for incoming data, the excess is stored in other parts of the computer's memory. Forcing this to happen can change the system's behavior, even inducing it to execute malicious code.

Attackers also trick users into installing malicious software—for example, by using deceptive e-mail messages containing links to bogus websites. And sometimes the attacks come from within: experts say that internal security policies are often lax or poorly implemented, giving people ample opportunity to steal from or sabotage their employers.

There have been some glimmers of hope. Many programs now install security updates automatically, without requiring user intervention. Antivirus companies have developed ways to recognize the characteristic behavior patterns of malware so that the system can respond more quickly to new breeds of infection. Cloud security providers have begun offering Web application firewalls, which filter Internet traffic before it's allowed to enter a victim's data center *(see "Threats Create Opportunities," p. 66)*.

However, many organizations don't keep abreast of these improvements. Applications for functions such as payroll are often custom-built and can't easily be upgraded to run on modern systems. Jeremiah Grossman, founder and chief technology officer of WhiteHat Security, a website risk management company based in Santa Clara, CA, estimates that up to a third of the Web is currently running on systems with known vulnerabilities.

Grossman says researchers are seeking creative solutions, such as systems that wrap outdated software in a protected layer or make it possible to do business safely on infected machines. But as long as new software is written, new vulnerabilities will keep surfacing. *—Erica Naone*

DATA SHOT

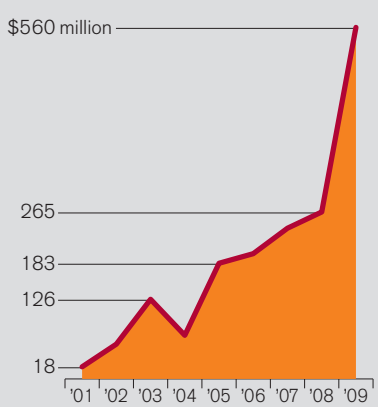
$575

The median loss per incident in the cyber crimes reported to U.S. government agencies in 2009; e-mail scams were responsible for most reports.

CRIME WAVE

More money is being lost to cyber crooks.

Annual losses of referred complaints



Source: Internet Crime Complaint Center

BAO FAN/IMAGINECHINA/AP; ALL CHARTS BY TOMMY MCCALL

INDUSTRY CHALLENGES

Measuring Security

There's really no way to compare two computers running two different operating systems, Web browsers, or any other type of program and definitively say which one is more secure. That makes it hard for governments and businesses to decide how best to spend money on security—or even how much they should spend in the first place. It's difficult to know whether a security product is effective or just has good marketing.

Consider virus scanners. They automatically examine files for malicious software, but they can only detect malware that's already been identified. So a scanner can't say that a computer system has zero viruses—it can just say that a system doesn't have any of the viruses the scanner was designed to catch. But unknown pieces of malicious code have been responsible for many of the most devastating attacks to date, including the much-publicized attack on Google earlier this year.

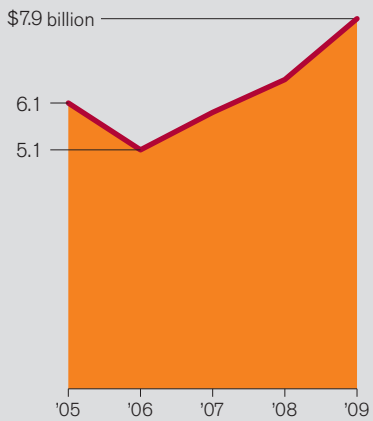
It used to be that there were surefire ways to know your system had been hacked. Files would be deleted; attackers would alter your website or make your system crash and ask for ransom. Today, however, the goal is to steal information or take control of a computer without tipping off users. Because many attacks go unnoticed, there are no truly reliable statistics about how many computers are compromised, let alone statistics that can measure the full economic impact of these intrusions.

And yet people are trying. Research projects at the Idaho National Laboratory, the U.S. Department of Defense–sponsored Institute for Defense Analyses, and MIT Lincoln Laboratory are all attempts to develop ways of measuring security. If these projects can successfully create a set of standardized metrics, it will be easier for companies that create good products to reap a return on their investments in research and development, rather than competing on a level playing field with those who simply have a huge marketing budget and those who are selling snake oil. In the meantime, the attackers gain ground. *—Simson Garfinkel*

MONEY WELL SPENT?

Spending on security is increasing, but is it too much—or too little?

Government spending on IT security



Source: Input

DATA SHOT

72%

The proportion of insiders caught committing cyber crimes who are not reported to law enforcement, according to a survey conducted by *CSO* magazine, the U.S. Secret Service, the CERT program at Carnegie Mellon University, and Deloitte.



Akamai's operations center can monitor attacks, but there is no definitive way of gauging how secure the network is.

COURTESY OF AKAMAI



Josh Abraham and Will Vandevanter are two of the experts who analyze security vulnerabilities for Rapid7.

CASE STUDY

Testing for Trouble

In the first two months of 2010 alone, 1,223 new vulnerabilities were added to the Open Source Vulnerability Database, a project designed to gather reports about security issues in all types of software. It's not unusual, then, for a company that relies on software to have thousands of vulnerabilities spread across various systems.

But there's a difference between a vulnerability and a real risk, says Corey Thomas, executive vice president of the Boston-based computer security firm Rapid7. If it's difficult for an attacker to exploit a vulnerability, Thomas says, then it doesn't amount to much of a threat.

Last year, Rapid7 acquired Metasploit, an open-source framework that tests systems for security holes, thus helping organizations separate threats from mere vulnerabilities. Metasploit's researchers and members of the open-source community use various strategies to stay on top of the vulnerabilities that attackers actually use, including watching news reports and monitoring systems designed to trap malware. The researchers can then create modules to see how systems would respond to an attack. Metasploit modules work the same way malicious software would, except that the user controls what the software does to the system after a breach is found. This lets users identify where they're at risk without suffering any damage.

Rapid7 maintains Metasploit as an entirely free, open-source project. It makes money by selling products that build on Metasploit or offering businesses additional services. But the very openness and easy availability of Metasploit modules suggest another problem. Rapid7 feared that acquiring Metasploit would cause a backlash from customers worried that the tool might help attackers. Thomas's argument is simple: "Do you want the information and knowledge to be accessible to you, or do you want it to be hidden and used by only the people who are malicious?"

Rapid7's first product based on Metasploit streamlines the testing process and makes it easier for nontechnical users to check their systems. Now the company will focus on creating more products to help customers identify the problems in their systems and fix them efficiently. —*Erica Naone*

POLICY

Global Gridlock on Cyber Crime

The first international treaty on fighting cyber crime went into effect six years ago. Called the European Convention on Cybercrime, it aims to make different country's laws compatible and promote investigative coöperation. But progress has stalled.

Just 30 nations, including the United States, have ratified the treaty. China and Brazil haven't even signed it. Most troubling is that Russia—which the Internet infrastructure company Akamai identifies as the leading source of computer attacks as of late 2009—has also refused to sign. Russia objects to a provision that would let foreign investigators bypass governments and work directly with network operators.

In the face of all these delays, criminal threats continue to evolve. Cloud computing, in particular, makes it easy to move data across borders and obscure the true origin of attacks. Some European politicians say that the European Union should create a cyber security czar. Other experts think countries should just work out agreements one on one.

CHRISTOPHER CHURCHILL

"We need to cut deals with countries we have problems with, not pursue a general convention which requires ratification in many countries," says Veni Markovski, who ran an Internet service provider in Bulgaria and is the representative to Russia from ICANN, the organization that assigns Internet domain names.

Representatives from the major nations have gathered several times recently for talks that could lead to bilateral agreements. Without one we're all less secure, because cyber criminals know they can wage attacks without getting caught, says Charles Barry, senior research fellow at the Center for Technology and National Security Policy at the National Defense University in Washington, DC. "Agreement among at least the major cyber players on what constitutes illicit behavior should be a high priority," he says. *—David Talbot*



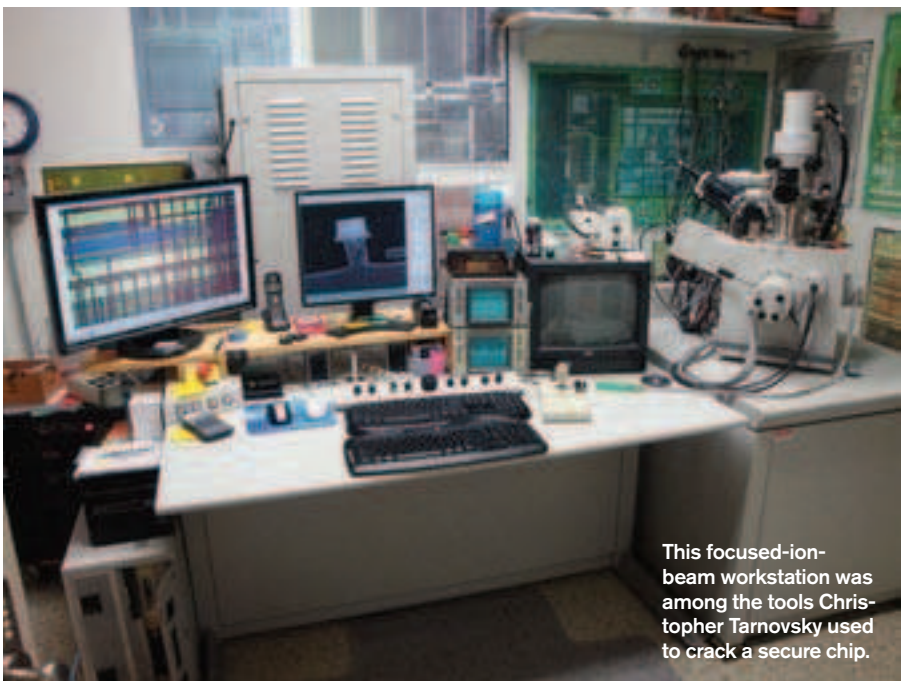
Cross-border cyber attacks suspected to originate from North Korea sparked bitter protests from South Koreans last year.

LEE JIN-MAN/AP (POLICY); COURTESY OF FLYLOGIC (RESEARCH)

DATA SHOT

1.8 billion

The number of attacks faced by Congress and government agencies in the United States every month.



This focused-ion-beam workstation was among the tools Christopher Tarnovsky used to crack a secure chip.

RESEARCH TO WATCH

Hope in Hardware

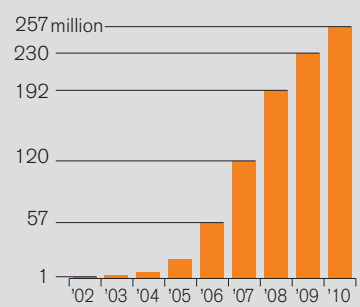
Since it's so hard to analyze the security of ever-changing software configurations *(see "Measuring Security," p. 61)*, many researchers are pursuing hardware-based security. They believe that hardware can be made simpler than software, is easier to verify, and is harder to hack once it's deployed.

One example of this strategy is the use of smart cards and USB tokens as an alternative to usernames and passwords. The U.S. Department of Defense uses such methods to control access to sensitive websites and to digitally sign and encrypt e-mail. Another approach is the Trusted Platform Module (TPM), a fingernail-size microchip that can be built into computers. An advantage of TPM is that the chips are already in many laptop and desktop computers, as well as in game consoles such as the Xbox 360. The modules give each of these systems an unforgeable serial number and a secure place to store digi-

SECURE BASE

Growing numbers of computers have security chips installed.

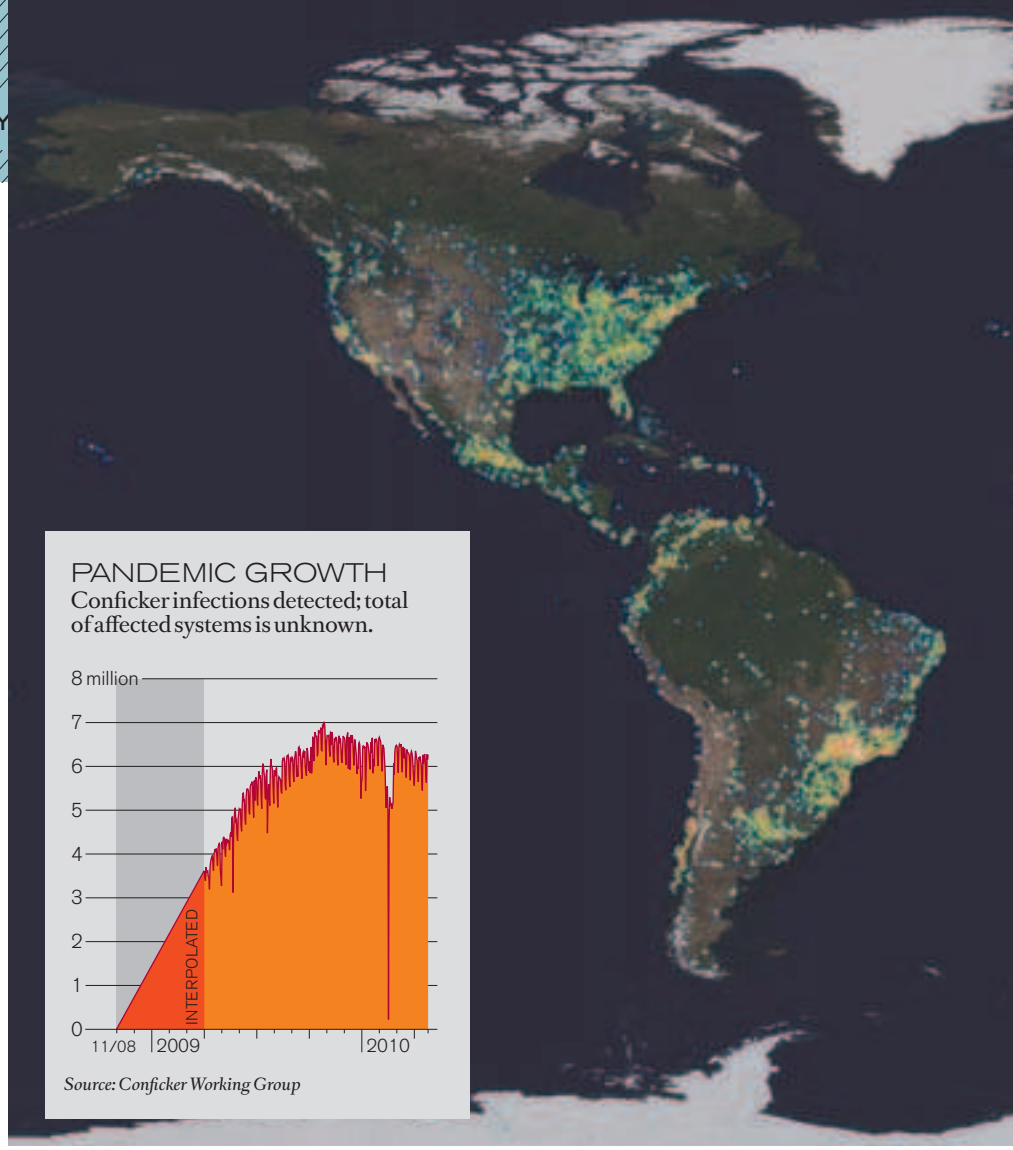
Trusted Platform Module shipments



Source: IDC

THE BIG PICTURE

Planetary Pestilence



The Conficker worm was first released in November 2008 and later followed up by increasingly sophisticated variants. Targeting a vulnerability in the Microsoft Windows operating system, the worm can spread by means of networks and USB flash drives. Millions of computers were rapidly infected; this map from security firm Team Cymru shows a snapshot of detected infections in January 2009. Since then, Conficker has proved difficult to eradicate. Its resilience is due in part to its ability to disable antivirus software, block users from accessing the websites of security vendors to get new software, and download encrypted updates designed to defeat countermeasures against previous versions of Conficker. Microsoft is offering a $250,000 reward for the identities of the worm's creators. —*Stephen Cass*

tal cryptographic keys, which can then be used instead of passwords.

Unlike smart cards and USB tokens, TPMs can also be used for something called "remote attestation," which lets a computer prove to another that its operating system hasn't been modified by a third party. And since TPMs are already widely deployed, they represent the best immediate hope for hardware-based security.

Unfortunately, relatively few applications take advantage of these modules, but people in both industry and academia are looking to change that. For example, MIT professor Srini Devadas and his students have shown how TPM microchips can improve security without requiring the operating system to be secure—an important step forward, since today's operating systems are too complex to be secured completely. Such a system might make online banking safer for consumers, for example. And last year researchers from the Technical University Munich in Germany showed how to use the modules with OpenID, an authentication protocol increasingly used by blogs and many of the smaller social-networking websites.

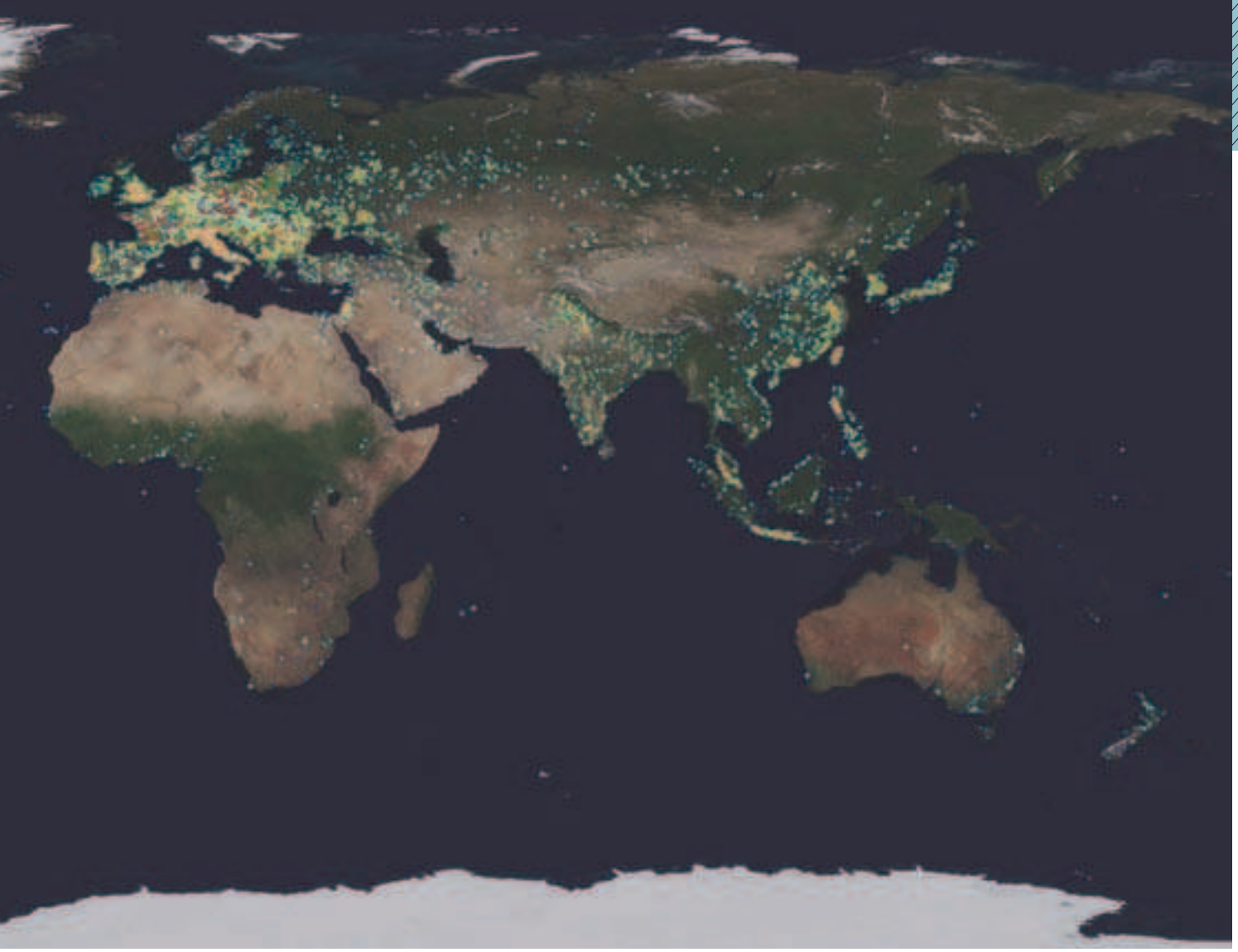
It takes a significant effort to crack the chips, as Christopher Tarnovsky, a former U.S. Army computer security specialist, demonstrated in February. By dissolving the chip's outer casing with acid, removing a protective inner mesh with rust remover, and tapping the communications channels with tiny needles, Tarnovsky was able to force a module to release its secret information. Such an attack might let someone who had stolen a laptop unlock remote websites or pose as the laptop's owner, but fortunately, it would be impractical to do this on a large scale. —*Simson Garfinkel*

DATA SHOT

1988

The year the first major computer worm was released on the Internet. The worm crashed systems at universities, hospitals, and military facilities. Its creator, Robert Morris, was fined $10,000.

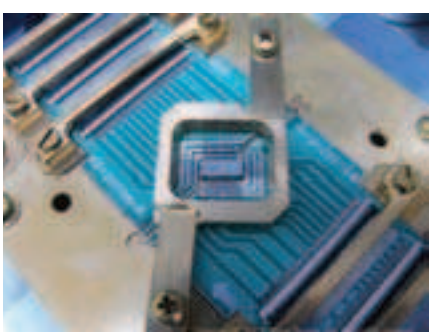
COURTESY OF TEAM CYMRU



OVER THE HORIZON

Bulletproofing Cryptography

Much of today's data security rests on encryption techniques involving mathematical functions that are easy to perform but hard to reverse, such as multiplying two large prime numbers. Factoring the result without knowing either of the prime numbers is very difficult, at least for the computers we use today; it could take thousands of years for even the most powerful supercomputer to identify the original numbers and crack an encrypted message.



D-Wave Systems says it is making significant progress toward developing quantum-computer hardware, such as this chip.

COURTESY OF D-WAVE SYSTEMS

The task would be a snap for a quantum computer, however. (In these computers, a bit need not be just a *0* or a *1*; it can exist in an infinite number of intermediate states.) A practical quantum computer is probably at least decades away, but simple demonstrations have already been made. Some researchers warn that such a computer would herald the death of encryption and expose not just new information but also preëxisting material encrypted in the expectation that it would stay secret indefinitely. Imagine if it became possible in 20 years to read electronic medical records being created today.

Alternative systems are being proposed. Lattice-based encryption, for example, relies on the difficulty of determining such things as the shortest vector possible in a given multidimensional lattice; that can be so hard it would stump even a quantum computer. Even though such a computer may not be available for many years, if ever, it's important to begin developing and deploying better cryptography now so it has time to diffuse throughout cyberspace. —*Robert Lemos*

MARKETWATCH

Threats Create Opportunities

A decade ago, a company looking to secure its computer systems would have purchased antivirus software, a firewall, and perhaps an intrusion detection system. Today, the growing variety of attacks has given rise to nearly 70 different security niches, including markets for firewalls that specifically protect Web-based applications and for systems that prevent data loss across an enterprise. Meanwhile, each submarket is getting increasingly complex. In 2009 one of the biggest security companies, Symantec, generated 2.9 million separate signatures, or digital patterns associated with malicious software—an increase of 71 percent over the previous year.

In response to this complexity, larger security firms have acquired many smaller firms. According to the 451 Group, an analysis firm, Symantec has spent $2.7 billion in the past three years to scoop up 10 companies, including the e-mail protection firm MessageLabs and the encryption provider PGP. McAfee acquired seven companies, including e-mail security firm MX Logic, for $1.1 billion during the same period. But the market remains fragmented: last year the top five security software companies accounted for 47 percent of the industry's revenues, down from 55 percent in 2007, according to the IT research company Gartner.



The labyrinth of modern security creates opportunities for companies offering managed security and cloud-based services. For example, experts from IBM or SecureWorks will, for a monthly fee, monitor a business's firewall logs, manage intrusion detection systems, block spam, and protect Web-based applications from malicious traffic. These kinds of services are getting more popular—especially cloud-based systems, which require no on-site hardware. A quarter of firms now outsource their e-mail filtering, and that number could grow to more than a third this year, according to Forrester Research.

The growing number of devices that connect to the Internet, from smart phones to electricity meters, creates yet another expanding market for security firms. In the past year, several rudimentary malicious programs have targeted iPhones and Android-based phones, and security researchers have released proof-of-concept programs, such as mobile botnets, that can take over mobile devices. Firms such as Lookout and Zenprise are already helping consumers and companies lock down their phones against the possibility of such attacks. Traditional antivirus firms are targeting this market as well. The market in security software for mobile devices is predicted to reach $4 billion by 2014, according to ABI Research. *—Robert Lemos*

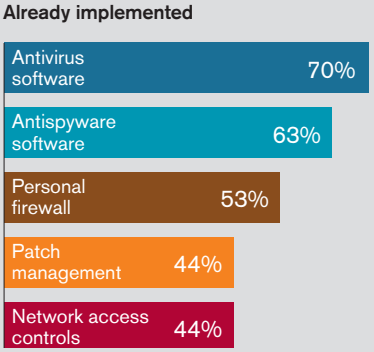
DATA SHOT

38%

The proportion of businesses surveyed by PricewaterhouseCoopers in 2009 that expected to increase spending on IT security over the next year—a six-point drop from 2008.

TOOLS OF THE TRADE

Popular security products used by small and medium-size businesses



Source: Forrester Research

SECURITY IP

Many of the acquisitions being made by larger security firms are driven by the desire to acquire the intellectual property of smaller firms. A good example is Symantec's acquisition of Brightmail in 2004: Brightmail owned three influential patents for e-mail filtering that have been widely cited by Microsoft, IBM, McAfee, and others. To explore IPVision's interactive analysis of these patents and their impact, go to **www.technologyreview.com/briefings/security.**

COURTESY OF MOTOROLA

COMPANIES TO WATCH: PUBLIC

Akamai

Operates a private data network

www.akamai.com
Founded: 1998
Management: Paul Sagan (CEO), Michael Afergan (CTO)
Employees: 1,750
Revenues: $859.8 billion
R&D: $43.7 million
Market cap: $6.9 billion

Technology: Akamai's security services are built on top of the software and hardware it uses for its private content delivery network. This network allows owners of high-traffic websites to mirror their content, such as video or Web applications, around the world for faster delivery to visitors. Because the company already inspects traffic as it passes through the network, adding on-demand security features for customers is relatively easy. Its Web application firewall, for example, can stop malicious attacks before they reach the customer's infrastructure. **Market:** Akamai expects that its security features will expand its market by allowing it to sell new products to existing customers, who work in sectors such as media, e-commerce, and financial services. **Strategy:** The company hopes that the reputation and resources it's built up around content delivery will attract customers interested in trying cloud-based security products—and that they'll eventually decide to purchase its content delivery services as well. **Challenges and next steps:** Akamai foresees difficulties integrating disparate services when customers use multiple security vendors. It plans to continue expanding its own range of in-house services.

Amazon

Sells cloud-based storage and processing

www.amazon.com
Founded: 1994
Management: Jeffrey Bezos (CEO), Andrew R. Jassy (senior vice president, Amazon Web Services)
Employees: 24,300
Revenues: $24.5 billion
R&D: $1.2 billion
Market cap: $55.9 billion

Technology: Aside from its large presence as an online retailer, Amazon is a provider of cloud computing services that offer on-demand storage and processing along with basic security. The company protects customers' data by maintaining backups, physically preventing unauthorized access to data centers, and stopping data from being intercepted as it travels through Amazon's infrastructure. **Market:** Amazon Web Services is best known for its appeal to startups and small businesses, since it allows them to avoid many of the capital costs involved in building infrastructure for things like hosting Web applications. But the company also offers its services to large organizations. **Strategy:** Amazon uses its cloud services to power and secure its own storefront, making the retail site a strong advertisement for its cloud services. The company plans to offer more elaborate services built on top of its basic processing and storage offerings. **Challenges and next steps:** Since security is a top concern for businesses reluctant to move into the cloud *(see "Security in the Ether," January/February 2010 and at technologyreview.com)*, Amazon must maintain the perception that it's able to safeguard its customers' data.

EMC

Owns a critical encryption technology

www.rsa.com
Founded: 1979
Management: Arthur Coviello (president, RSA), Bret Hartman (CTO, RSA)
Employees: 43,200
Revenues: $14.0 billion
R&D: $1.6 billion
Market cap: $38.3 billion

Technology: RSA is EMC's security division. Its core technology is the RSA algorithm, which is used worldwide to encrypt sensitive information sent over the Internet. It uses a technique in which two parties who wish to communicate can openly exchange so-called public keys; anything encrypted with a public key can only be decrypted by each party's corresponding private key. RSA also offers products that watch corporate systems for evidence of malware activity. **Market:** RSA has more than 9,000 customers worldwide. The company focuses on providing a broad set of Internet security tools, including authentication, which allow its customers to verify transactions and communications that occur online. **Strategy:** RSA's parent company, EMC, is eyeing the growing importance of cloud computing services and developing its own offerings in this market. The company hopes that integrating its security expertise into its overall cloud business will increase customers' confidence in the products. **Challenges and next steps:** An attack on its algorithm by academic researchers gained attention earlier this year, but this type of attack currently requires a huge investment of time and resources, so it is not a practical threat, at least for now.

F-Secure

Specializes in security software for smart phones

www.f-secure.com
Founded: 1988
Management: Kimmo Alkio (CEO), Pirkka Palomäki (CTO)
Employees: 720
Revenues: $179.2 million
R&D: $40.1 million
Market cap: $396.0 million

Technology: F-Secure offers products such as antivirus and antispyware software. The Finnish company's mobile security products, designed to protect against malware infection on smart phones, are based on a database of all known mobile malware. **Market:** F-Secure moved into the mobile market early and has captured the lion's share of it through deals with companies including Vodaphone, T-Mobile, Orange, and Nokia. It also sells security products for personal computers. **Strategy:** F-Secure focuses on providing products and services that operators can resell. The strategy has worked particularly well with mobile operators, but the company has also tried it on the PC side with broadband operators. F-Secure says it has more than 200 partnerships with operators globally. **Challenges and next steps:** The company believes that building add-on firewall or antivirus products is reaching its limit of effectiveness; now it is looking to incorporate its security software throughout operating systems and applications. It also believes that cyber attackers will shift their attention to new targets. Securing location information derived from smart phones, for example, is a growing challenge.

Google

Building a more secure operating system

www.google.com
Founded: 1998
Management: Eric Schmidt (CEO), Sergey Brin (CTO)
Employees: 19,835
Revenues: $23.7 billion
R&D: $2.8 billion
Market cap: $161.0 billion

Technology: Google's Chrome browser makes extensive use of a technique known as sandboxing, in which operations that handle Web pages can't access the local system. Google is also developing an operating system called Chrome, which uses cloud technology to stay secure. Chrome OS is designed to check itself periodically to search for any differences between the software installed on a user's machine and Google's official version. Because the operating system is designed to store its data in the cloud rather than on the machine, it can be reinstalled without inconveniencing the user if anomalies are detected. **Market:** Businesses and consumers whose computer use revolves around a Web browser. **Strategy:** Google believes that its browser and operating system will encourage users to spend more time online, potentially using more of the company's services. It also hopes its products will push other vendors to make products that improve the online experience for everyone. **Challenges and next steps:** Google has also introduced a program to pay researchers if they find significant security vulnerabilities in the Chrome browser. It has not yet announced a release date for Chrome OS, but the underlying code has been released to the open-source community.

COMPANIES TO WATCH: PUBLIC

Hewlett-Packard

Pays researchers a bounty for security information

www.tippingpoint.com
Founded: 1939
Management: Alan Kessler (president, TippingPoint), Dave Larson (vice president, integrated product strategy)
Employees: 304,000
Revenues: $114.6 billion
R&D: $2.8 billion
Market cap: $111.4 billion

Technology: HP's TippingPoint division sells an intrusion prevention system. It features "virtual software patch" technology, which offers protection for vulnerabilities in products that haven't yet been patched by the vendors. Partly to gain information for this service, TippingPoint runs the Zero Day Initiative, which purchases information on vulnerabilities from security researchers. **Market:** Tipping Point sells its services primarily to corporate enterprises, government agencies, service providers, and academic institutions. **Strategy:** The Zero Day Initiative gives TippingPoint a chance to offer a product that protects against vulnerabilities before they're publicly known. The initiative has also brought notoriety and visibility to the company through bug-finding contests such as Pwn2Own, which attract top security researchers from around the world. **Challenges and next steps:** The Zero Day Initiative's model of paying researchers for information about vulnerabilities is uncommon in the industry. Criminals have long been willing to buy such information, but creating a legitimate market for it is new. TippingPoint must prove that the system works economically and fend off controversy about it.

McAfee

Building a one-stop shop for computer security

www.mcafee.com
Founded: 1987
Management: David DeWalt (CEO), George Kurtz (CTO)
Employees: 6,100
Revenues: $1.9 billion
R&D: $324.4 million
Market cap: $5.2 billion

Technology: McAfee offers a wide variety of security products, but its flagship is a unified platform that ties together the company's research into cyber threats, computer and network security products, and risk and compliance capabilities. The company also offers other integrated systems on a software-as-a-service basis. **Market:** McAfee targets diverse customers, offering products aimed at consumers, small businesses, midsize companies, and large corporations. **Strategy:** The company hopes that the breadth of its product line will make it attractive to companies looking for comprehensive security services that can be controlled through a single interface. **Challenges and next steps:** In addition to threats from companies such as Symantec and Trend Micro, McAfee faces competition from smaller companies that offer similar products at much lower or zero cost. The company is concerned that the trend toward netbooks and other inexpensive computing technologies may indicate customers' willingness to emphasize price above functionality. If that's the case, the competitors will have an advantage. A recent snafu in which an update damaged users' machines showed that McAfee is vulnerable to negative publicity.

Microsoft

Its popular software is a favorite target for hackers

www.microsoft.com
Founded: 1975
Management: Steve Ballmer (CEO), Craig Mundie (chief research and strategy officer)
Employees: 92,736
Revenues: $58.4 billion
R&D: $9.0 billion
Market cap: $235.4 billion

Technology: The company has developed a range of antimalware defenses to make its operating systems more secure. It has introduced programs such as End to End Trust, an attempt to develop technologies that can contribute to a more secure Internet. **Market:** Microsoft's products have captured a broad segment of the market and are particularly popular with enterprise customers. Its browser, Internet Explorer, is used by more than half of Internet users worldwide. **Strategy:** Microsoft's Trustworthy Computing initiative began in 2002, and its products' reputation for security has been slowly improving ever since. However, the company feels there's a limit to what can be accomplished by focusing on technical improvements to individual products. It looks to the End to End Trust initiative to address Internet security issues that are beyond its direct control. **Challenges and next steps:** Microsoft will remain the primary focus of attention for cyber attackers. Many users are often slow to upgrade to new versions of its products, making it hard for the company to roll out improved security technologies. For its existing platforms, Microsoft is trying to educate third-party developers to design security into Windows applications from the start.

Symantec

Relies heavily on partnerships to distribute its products

www.symantec.com
Founded: 1982
Management: Enrique Salem (CEO), Mark Bregman (CTO)
Employees: 17,400
Revenues: $6.2 billion
R&D: $880.0 million
Market cap: $11.7 billion

Technology: In addition to the antivirus software for which it is best known, Symantec offers products for security, backup and recovery, storage, compliance, and systems management. **Market:** While Symantec sells many products directly, it also offers them through other companies, such as Internet service providers and computer manufacturers. The company says it maintains partnerships with about 40,000 companies worldwide. **Strategy:** Symantec is expanding from products that are delivered as services or installed as add-on appliances in customers' data centers. The company believes that security is beginning to converge with storage and systems management, and it is focusing on creating integrated products that draw on its expertise in these different areas. **Challenges and next steps:** Because Symantec's strategy calls for a great deal of coöperation with partners such as computer manufacturers, the company faces challenges from other vendors that make similar software. If Symantec does happen to lose its relationship with a manufacturer to another security vendor, it will have to continue developing its products without the benefit of its special access to end users.

Trend Micro

Targets small businesses

www.trendmicro.com
Founded: 1988
Management: Eva Chen (CEO), Oscar Chang (chief development officer)
Employees: 4,434
Revenues: $1.0 billion
R&D: N/A
Market cap: $3.9 billion

Technology: Trend Micro sells antivirus, antispam, and network security software for businesses and consumers. It has recently developed a cloud-based system to identify and stop threats as they emerge. The company is also developing services for companies hoping to protect information they've stored in clouds. **Market:** Two-thirds of the Tokyo-based company's worldwide revenue comes from business customers, and the remaining third from consumers; about 40 percent of its sales come from Japan. **Strategy:** The company is expanding its global presence. It has also grown by acquiring several companies working in the antispam, antispyware, encryption, and data-center security arenas. It has focused recently on offering products aimed at small businesses, which lack both the legal protections afforded to consumers (such as protection from credit card fraud) and the resources that larger companies can bring to bear against cyber crime. **Challenges and next steps:** In order to keep up with the increasing sophistication of cyber criminals, Trend Micro is moving to add various products designed to protect virtualized environments and data centers and to protect access to data as it moves across the Internet.

COMPANIES TO WATCH: PRIVATE

Facebook

Guarding users' data

www.facebook.com
Founders: Mark Zuckerberg, Chris Hughes, Dustin Moskovitz, Eduardo Saverin
Management: Mark Zuckerberg (CEO), Sheryl Sandberg (COO)
Funding: Over $700 million
Key investors: Peter Thiel, Accel Partners, Greylock Partners, Digital Sky Technologies

Technology: As Facebook has grown and become a more frequent target of attacks, the company has developed strategies for protecting users' data, even when it can't control whether their machines are infected with malware. For example, the company can deactivate links shared on the site if they turn out to be malicious, and it works with major vendors to patch applications. **Market:** Through partnerships that Facebook is developing with marketers, the large amounts of data it has collected on its customers will be used to advertise to them. **Strategy:** The company, which works to establish itself as a trusted site, benefits from the network effect of the millions of people who already use its service. Facebook has also developed defenses to prevent malware from being delivered to users through the applications that it hosts from third-party developers. **Challenges and next steps:** Facebook is under increasing pressure to secure the customer data it has collected. In particular, the company must enhance the security of the interfaces that allow other sites to tap into that information. The company came under fire recently after a number of security vulnerabilities were found in its new Open Graph platform, which allows third-party sites access to user data.

Flylogic Engineering

Researches vulnerabilities in hardware

www.flylogic.net
Founders: Christopher Tarnovsky
Management: Christopher Tarnovsky (principal)
Funding: Self-funded

Technology: Flylogic's expertise lies in breaking a device's physical defenses in order to extract the information stored inside, allowing the company to identify vulnerabilities and advise customers on better designs. The company employs tools that allow a user to look deep into the architecture of a chip and perform fine-grained operations on it. Once this tool reveals how to get into the integrated circuit, Flylogic is often able to come up with a simpler way to crack the chip. **Market:** The company targets both chip makers and the manufacturers of devices with embedded chips, such as cell phones and smart cards. **Strategy:** The relationship between hardware manufacturers and security consultants is still largely adversarial. Flylogic's strategy is to carefully publicize some of the vulnerabilities it finds while working with manufacturers to help them improve. The company hopes to establish repeat business with major chip manufacturers. **Challenges and next steps:** Chips are growing smaller and more complex. But for the most part, these changes have occurred without taking security into account. Flylogic must continue developing new techniques for dealing with smaller physical devices while building positive relationships with manufacturers.

Independent Security Evaluators

Performs high-end security analysis

securityevaluators.com
Founders: Avi Rubin, Stephen Bono, Matthew Green, Adam Stubblefield
Management: Avi Rubin (president)
Funding: Self-funded

Technology: The company employs experts capable of extensive, hands-on analysis of systems security. Its consultants have been responsible for feats such as finding early bugs in the iPhone and Android platforms, electronic voting machines, and Blu-ray and HD-DVD players, as well as flaws in an early encryption protocol used to secure wireless access points. The company has developed specialized tools for testing system security, but it uses them internally rather than selling them to customers. **Market:** Independent Security Evaluators has business units focused on three areas: enhancing network security, providing technical support to law firms, and testing software in the absence of information about its underlying architecture. **Strategy:** The company has positioned itself at the high end of security analysis. It tells customers that by hiring experts as good as any would-be attacker, it can analyze their systems and eliminate weaknesses before outsiders can find them. **Challenges and next steps:** The company has been primarily concerned with technical rather than financial issues; it currently has only one manager. It is now examining how to grow past its current size without changing its technically focused culture.

IOActive

Uncovers security flaws in infrastructure

www.ioactive.com
Founders: Joshua Pennell
Management: Jennifer Steffens (CEO), Dan Kaminsky (director of penetration testing)
Funding: Not disclosed

Technology: IOActive's staff has been responsible for several high-profile discoveries of security vulnerabilities, including one in the Internet's fundamental structure: its experts helped find and patch a flaw in the domain name system, which is responsible for matching the URLs that users type into their browsers with the corresponding numeric addresses used to route traffic. More recently, IOActive's experts analyzed and found vulnerabilities in the design of the infrastructure for a smart electrical grid. They also demonstrated an attack that could spread malware throughout the grid, potentially causing a massive power outage. **Market:** The company has customers in a variety of market segments, including power, games, hardware, finance, travel, and social networking. **Strategy:** IOActive recruits big names on the security speaker circuit and builds its reputation on their discoveries. **Challenges and next steps:** IOActive must walk a careful line in order to publicize its achievements without alienating the companies it hopes to win as customers. For example, when the company revealed problems it uncovered with smart electricity meters, its experts did not name any specific brands affected.

Ksplice

Lets system administrators install security patches without downtime

www.ksplice.com
Founders: Jeff Arnold, Tim Abbott, Waseem Daher, Anders Kaseorg
Management: Jeff Arnold (CEO), Tim Abbott (CTO)
Funding: Self-funded

Technology: For customers, rebooting after installing security updates is annoying; for companies, the downtime can be costly, in terms of lost internal productivity, lost customer sales, or both. Ksplice's technology, which works with the Linux operating system that many businesses use to run servers, allows security updates to be converted into a form that can be installed without rebooting. The technology works by analyzing the effect an update would have on a system. A Ksplice patch then makes those changes without disrupting other processes needed to keep the system running. **Market:** Ksplice is currently targeting infrastructure providers, companies that offer cloud computing services, and Web hosting companies. **Strategy:** The company intends to build its business foundation on companies that use Linux, but the long-term vision is to extend its technology to handle middleware and application software above the level of the operating system. **Challenges and next steps:** Ksplice began as a very small startup and is now expanding. It has previously been interested in establishing partnerships with the companies that issue security updates, which would allow it to serve a much larger portion of the market.

COMPANIES TO WATCH: PRIVATE

Panda Security

Creates cloud-based security products

www.pandasecurity.com
Founders: Mikel Urizarbarrena
Management: Juan Santana (CEO), Rick Carlson (president, Panda Security U.S.)
Funding: $13.8 million
Key investors: Investindustrial, Gala Capital, HarbourVest, Atlantic Bridge

Technology: Most antivirus products work by storing virus signatures on users' machines; matching these signatures against Internet traffic or files on storage devices allows the software to recognize threats when they appear. Panda's products store and analyze signatures in the cloud. This means signatures can be kept up to date more easily, and users' computers aren't slowed by the computational demands of the analysis. **Market:** Panda is currently strong in the U.S. small-business market, where its services are particularly appealing because they're low cost and don't require customers to maintain any infrastructure. The company foresees increasing interest in managed services in this market. **Strategy:** Panda hopes the shift to cloud computing will help it pick up market share. A key part of the company's strategy is to give away its cloud antivirus product to consumers. Not only has this helped build worldwide name recognition, but it allows the company to collect information about the behavior of malware on a global scale. **Challenges and next steps:** Panda is working to expand globally. In order to accomplish this, it must take on bigger antivirus companies with more established names.

Rapid7

Helps companies identify their most dangerous vulnerabilities

www.rapid7.com
Founders: Tas Giakouminakis, Chad Loder, Alan Matthews
Management: Mike Tuchen (CEO), Tas Giakouminakis (CTO)
Funding: $9 million
Key investors: Bain Capital Ventures

Technology: Rapid7's NeXpose scans customers' networks, databases, and Web applications systems, identifying vulnerabilities and ranking their severity. The Metasploit Framework, a popular open-source platform that it recently acquired, allows customers to do their own testing to identify the system flaws that attackers can actually exploit. Metasploit is known for maintaining a large database of public, tested exploits. **Market:** The company is focused on selling to the security officers of medium to large companies. By diversifying its products, it hopes to build customer loyalty in a confusing market for security services. **Strategy:** Rapid7 feels that the security industry has credibility issues: customers are overwhelmed by an array of products and uncertain about which vulnerabilities deserve their attention. The company's strategy is to help customers identify and mitigate the risks that have the biggest impact on their business. **Challenges and next steps:** The company is now seeking to make its security products more accessible and easier to use. To that end, it has been releasing products such as Metasploit Express—a low-cost, packaged version of the Metasploit Framework.

Trusteer

Sells tools to financial institutions to prevent fraud

www.trusteer.com
Founders: Mickey Boodaei
Management: Mickey Boodaei (CEO), Amit Klein (CTO)
Funding: $14 million
Key investors: U.S. Venture Partners; Shlomo Kramer, CEO of Imperva

Technology: Malware infecting users' machines often tries to access sensitive data as it flows through the user's browser. Trusteer provides technology that companies, particularly banks, can use to protect their customers. A recently launched service, Flashlight, provides tools that banks can use to identify the exact piece of malware responsible for any incidents that occur, easing the process of investigating breaches and helping companies improve their defenses. **Market:** The company is currently focused on providing fraud prevention services to financial institutions, but it also has products aimed at home users and at other businesses concerned about fraud. **Strategy:** Traditionally, different companies have provided different types of fraud prevention products: some focused on consumer products that protect the user's desktop, and others focused on protecting vendors' systems. Trusteer hopes to bridge the two services, providing a more comprehensive defense against fraud. **Challenges and next steps:** Trusteer intends to expand its line of fraud prevention products for online service providers. It hopes to diversify beyond the financial sector, looking at ways to prevent fraud in other types of enterprises.

Verdasys

Develops security designed to defend against insider attacks

www.verdasys.com
Founders: Seth Birnbaum, Allen H. Michels, Nicholas Stamos, Tomas Revesz
Management: Seth Birnbaum (CEO), Dan Geer (VP and chief scientist emeritus)
Funding: Self-funded

Technology: Verdasys's software protects systems by inserting itself deeper into the operating system than most attackers can reach. From that position, it's able to assess all attempts to access data on the machine or device. If the attempt doesn't meet the criteria laid out by corporate policy, the software blocks it. **Market:** The company focuses on protecting the data of top-tier global companies. It has strong operations in China and Taiwan and is moving into the European market, specifically Germany and France. **Strategy:** Verdasys started out by trying to protect companies against threats from their own employees. However, many attacks from outside happen when bad actors are able to pose as insiders or steal credentials. The company is now working to offer data protection of all kinds. **Challenges and next steps:** Customers are tired of buying a bunch of separate security products. Like others, Verdasys is working to integrate a variety of protections into its own products, both by expanding its technology and by figuring out how that technology can work in conjunction with, for example, advanced malware detection. The company is also planning its first product that will support Macs.

WhiteHat Security

Securing Web applications

www.whitehatsec.com
Founders: Jeremiah Grossman
Management: Stephanie Fohn (CEO), Jeremiah Grossman (CTO)
Funding: $13.2 million
Key investors: Altos Ventures, Garage Technology Ventures, Horizon Ventures, Startup Capital Ventures

Technology: WhiteHat provides a software-as-a-service approach to Web application security. Its platform identifies and manages website vulnerabilities and can be integrated with other security technologies to protect websites. **Market:** The company focuses on highly regulated segments of the market, such as financial companies, e-commerce, and health care. **Strategy:** WhiteHat has been establishing partnerships to provide its services through other businesses. For example, a recent deal with Verizon will bring its software to the telecommunications giant's customers. **Challenges and next steps:** Web applications are popular targets; the company estimates that 75 to 80 percent of attacks on businesses come through this conduit. WhiteHat must stay on top of new trends while developing its distribution channels to fend off competition from companies such as HP and IBM. Securing websites is complicated by a divide between security teams and website development teams, which often don't report to the same managers in a company. Often, security problems are identified but not resolved. To differentiate itself, WhiteHat is trying to make it as simple as possible for companies to act on the information about vulnerabilities that it provides.

Get it Today!

Introducing the new iPhone app from Technology Review



Access daily news, watch award-winning videos, listen to audio playlists and much more. Get it today!

Download for free at **www.technologyreview.com/app**

REVIEWS

TELECOM

America's Broadband Dilemma

CAN THE FCC BRING ACCESS TO EVERYONE IN THE COUNTRY AND ACHIEVE WORLD-LEADING SPEEDS AT THE SAME TIME?

By BOBBIE JOHNSON

For millions of people around the world, broadband Internet access is big part of modern life. We download movies and music, play online games, share photos, and upload information to social-networking sites—all at ever-increasing speeds. Rates of at least 50 megabits per second—enough to download a DVD-quality movie in about 10 minutes—have become mainstream in cities from Seoul to Stockholm. In the United States, however, the broadband landscape is different: the average download speed is about 10 megabits per second, according to the broadband testing firm Ookla, and only 23 people in 100 have broadband subscriptions, according to the International Telecommunications Union *(see "The Global Broadband Spectrum," p. 24)*. Statistics from the Organization for Economic Coöperation and Development rank the United States behind more than a dozen other countries—including South Korea, Japan, Canada, the U.K., Sweden, and Belgium—in both broadband penetration and average advertised speed.

Faced with these statistics—and the widespread assumption that access to high-speed broadband is critical to the country's economic health—the U.S. Federal Communications Commission created the National Broadband Plan, which directs up to $15.5 billion in public funds toward improving U.S. connectivity. The plan aims not only to ensure affordable and reliable broadband for every community but also to equip the majority of households (some 100 million homes) with lines running at speeds of at least 100 megabits per second. It's an attempt to shove the United States into the high-speed age—and all of it, the FCC suggests, is achievable by 2020.

THE NATIONAL BROADBAND PLAN
FCC
www.broadband.gov/plan/

Yet the case for federal investment boils down to one fundamental question: how much public good will $15.5 billion buy? Answering that with any accuracy, it turns out, is nearly impossible. Serious studies on the economic and social effects of wider, faster Internet access are surprisingly few—and many of those that do exist are dated. The answer also depends on how the FCC balances the plan's two goals of inclusivity and innovation.

It is often taken for granted that greater access to high-speed Internet services will boost the economy while improving health care, education, civic engagement, and more. Such assumptions are built into the plan and endorsed by various experts. In March of last year, for example, the Information Technology and Innovation Foundation, a think tank in Washington, DC, published a study suggesting that government support for wired and wireless broadband is vital to future economic development. The benefits of increased Internet access, the report's authors suggested, in turn spur the growth of new networked technologies as well as wholly unforeseen developments.

But Shane Greenstein, a professor of management and strategy at Northwestern University's Kellogg School of Management, says the advantages are in fact far less obvious. "The research challenge is substantial," says Greenstein, one of a handful of academics who have studied the economic impact of broadband. "One problem is that the real impact generally doesn't come in the sector where the investment takes place. For example, when broadband first arrived, who knew that restructuring the music industry would be the first thing to happen?" A lack of empirical research, Greenstein suggests, is also the result of a kind of institutional blindness apparent on nearly every side: "It's in no one's interest to be a skeptic, because it undermines one of the mythologies of broadband—that it is a technological panacea."

A 2007 study by researchers at MIT and at another Washington think tank, the Brookings Institution, did find some benefits when it attempted to discern the effect of increased broadband penetration on job opportunities at a state level. More high-speed access barely seemed to change activity in sectors such as construction, but it appeared to improve opportunities in knowl-



MARIO WAGNER

edge industries like finance, education, and health care. The researchers determined that each percentage-point increase in broadband penetration was associated with an overall employment increase of 0.2 percent to 0.3 percent. William Lehr, an economist at MIT and one of the paper's authors, says that the returns diminish as penetration nears the FCC's target of 100 percent, but the advantages remain significant.

It's less clear, however, whether the superfast connections championed by the FCC offer benefits commensurate with the costs. A study published last year by Motu Economic and Public Policy Research, a nonprofit institute in New Zealand, found that increasing broadband speeds may not help businesses' bottom lines. The research, which examined 6,000 companies, found that productivity increased significantly when service was upgraded from narrowband to broadband; but there was "no discernible additional effect arising from a shift from slow to fast broadband."

Nonetheless, the FCC does want commercial speeds to increase rapidly, to help the United States keep pace with rival countries. At the same time, the National Broadband Plan articulates a social and moral imperative to make sure that everybody can access the same basic services and operate in a 21st-century economy. Indeed, the plan often conflates these two goals. But the truth is that they require different technical approaches, political policies, and levels of investment.

The challenge, then, is to work out how to balance inclusion with innovation on a budget of $15.5 billion. Guidelines that the European Commission published last October after reviewing projects across the continent suggest that heavy government investment is the best way to extend broadband to underserved areas. That could be expensive, however. Northwestern's Greenstein points out that bringing broadband to the farthest reaches of the United States will come at rapidly increasing costs—as much as $5,000 per household in some rural parts of the country, compared with a couple of hundred dollars in built-up areas.

Instead, the FCC recommends a fresh approach: freeing up new portions of the wireless spectrum and encouraging mobile broadband providers to fill the gaps in coverage. Some academics have endorsed this solution, but wireless broadband technologies are unproved. WiMax, for example, can deliver speeds of 50 megabits per second, but that speed declines with distance from the transmitting station.

Achieving ever-higher speeds may also require significant government interven-

tion. According to a study by Harvard University's Berkman Center for Internet and Society, the key to speeding up existing service is an initial government investment combined with policies that encourage competition. Municipal investment in fiber networking capacity, which is then leased to commercial parties, has led to increased broadband speeds in European cities such as Amsterdam and Stockholm. But it will be tricky to follow this path in the United States, because the industry has been set up differently. In the 1990s, the FCC decided to encourage competition between infrastructures such as cable and DSL, rather than between different providers using a shared backbone. As a result, companies in the United States have been less willing to shoulder the cost of investing in new broadband technology, since doing so would give them little advantage over any direct competitor.

Yet private investment will be vital to increasing broadband speeds. Korea's rapid advances in the past decade were attributable in no small part to funding from companies. And there are encouraging signs that something similar is beginning to happen in the United States; in the most obvious example, Google is planning to roll out one-gigabit-per-second fiber lines to at least 50,000 and up to 500,000 people in trial locations across the country. But an FCC task force has suggested that more than $300 billion of private funding would eventually be required on top of the government's expenditure in order to boost speeds to 100 megabits per second or higher for the entire nation.

In the end, the success of the National Broadband Plan will be judged according to the targets that the FCC has set for increasing both penetration and speeds by 2020. But the tension between those two distinct goals leaves a desirable outcome very much in doubt. TR

BOBBIE JOHNSON IS A FREELANCE WRITER BASED IN SAN FRANCISCO. PREVIOUSLY, HE WAS THE TECHNOLOGY CORRESPONDENT FOR THE *GUARDIAN* NEWSPAPER.

BIOMEDICINE

The Argument over Aging

A DRUG TO EXTEND GOOD HEALTH AND POSTPONE DECLINE IS ON THE HORIZON, SOME RESEARCHERS SAY. OTHER DON'T BELIEVE IT.

By KAREN WEINTRAUB

Sirtris Pharmaceuticals was, until recently, the golden child of antiaging research. Founded by Harvard biochemist David Sinclair and venture capitalist Christoph Westphal, it produced research suggesting something almost too good to be true: that a chemical in red wine could help you live a longer, healthier life. With its young, photogenic founders, the startup was a media darling, the subject of dozens of breathless magazine and newspaper articles. Pharmaceutical giant GlaxoSmithKline was so impressed that it spent $720 million to buy Sirtris in 2008.

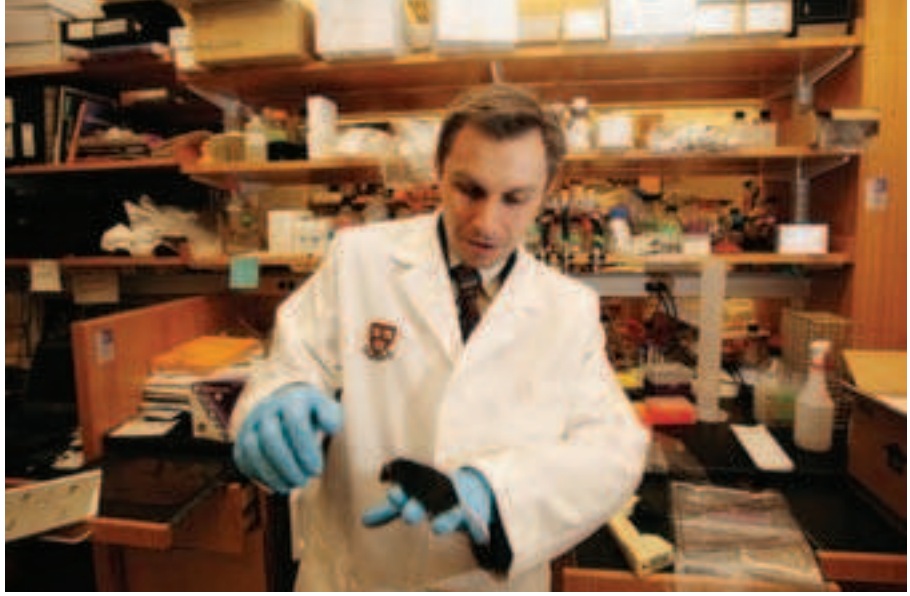
THE YOUTH PILL
David Stipp
Current, 2010

David Stipp's new book *The Youth Pill* traces this meteoritic rise and other events in the history of antiaging research, detailing how the science and personalities came together at just the right moment to create the successful company. In the mid to late 1990s, Stipp explains, what had been considered a fringe field began evolving into a focused attempt to uncover the biochemistry of aging. Scientists including Cynthia Kenyon at the University of California, San Francisco, and Leonard Guarente at MIT began to find genes linked to longevity in lower organisms such as yeast and worms, prompting a conceptual shift in our understanding of aging. Rather than inevitable decay, their work suggested, aging was a genetically controlled process—and thus one that could be manipulated.

Sirtris was one of the companies to emerge as this view of aging gained currency. At the heart of its drug development program are a class of enzymes called sirtuins: the molecular signals that they send appear to silence aging-related genes during times of starvation. The sirtuins' role in aging was first identified in 1993 by Guarente and his colleagues. (Sinclair would later join the lab as a postdoc.) As Stipp explains, the role of these enzymes in aging made sense to scientists who had known for years that caloric restriction, or nutritionally adequate diets about 30 percent lower in calories than average, could extend the lives of yeast, worms, and mice (the effect was also later demonstrated in rhesus monkeys). Realistically, however, few people can stick to this type of diet. So for more than a decade, the primary goal of antiaging researchers has been to mimic caloric restriction with a pill, a prospect that Stipp describes as "the great free lunch." Such a drug, he writes, would theoretically postpone aging in people, extending their years of good health and limiting their years of decline.

In 2003, Sinclair made headlines around the world when he announced that the red-wine component resveratrol, which had previously been linked to a reduction in heart disease, extended life span in yeast. He argued that the compound activated one of the sirtuins and proposed that it mimicked the effects of caloric restriction. Sinclair and Westphal launched Sirtris in 2004 with the aim of developing molecules that could stimulate the enzyme much more potently. The company is developing treatments not for aging itself—which the U.S. Food and Drug Administration doesn't consider an illness—but for diseases of aging, such as diabetes, Alzheimer's, and cancer.

As Stipp recounts, hopes for antiaging drugs captured media attention and investors' imaginations. But a different con-



RICK FRIEDMAN/WPN

LONGEVITY LAB Harvard's David Sinclair is testing compounds in mice that could be used to slow down the aging process in humans.

versation has played out in the academic community. Some scientists doubted whether resveratrol truly targeted the sirtuins. Researchers at drug maker Pfizer also published a study in January questioning whether one of Sirtris's newer compounds targets the enzyme. The study failed to confirm the health benefits seen in earlier trials. To make matters worse, safety concerns have arisen over one of Sirtris's resveratrol compounds. In May, Glaxo announced that it would not expand a clinical trial for multiple-myeloma patients until it better understood why some participants developed a dangerous kidney ailment.

The field of antiaging research is littered with failures, and the controversy over Sirtris's compounds highlights just how difficult it has been to transform exciting scientific discoveries about the aging process into useful drugs. As Stipp illustrates, many candidates with promising antiaging benefits later failed to work in mammals or showed conflicting results.

Elixir Pharmaceuticals, which was cofounded by Kenyon and Guarente in 1999 to translate their findings on the genetics of aging into a pill, was once "the leading commercial effort to turn research on aging into antiaging drugs," says Stipp. But the company has been far less successful than Sirtris in generating funding and excitement; today it employs just a handful of people, who are still pursuing sirtuins but have also moved on to developing other types of drugs. (Both Kenyon and Guarente have since left Elixir. Guarente joined Sirtris's scientific advisory board in 2007.) Peter S. DiStefano, chief scientific officer of Elixir, is no fan of the rival company, accusing it of weak science and overzealous claims. "While Sirtris was way more successful than Elixir from a business perspective, at least I have my scientific integrity and can look at myself and say I did the right thing the right way," he says.

Even if Sirtris's compounds don't pan out as safe, effective drugs, the enzymes behind them have great medical potential, says Matt Kaeberlein, an assistant professor in the pathology department at the University of Washington, who is another former student of Guarente's and a consistent critic of some of Sinclair's work. These enzymes have been highly conserved through evolution, appearing in worms, flies, mice, and primates, and they play a central role in the biochemistry of the cell. Guarente says, "If the whole world gave up on sirtuins, I would still start another company for the next generation of sirtuin drugs based on what I know."

But some scientists doubt that sirtuins hold the key to life extension; for one thing, sirtuin activation hasn't been shown to extend life in healthy animals. A number of other molecular mechanisms are also under close scrutiny for their effects on aging. Kenyon, director of the Hillblom Center for the Biology of Aging at UCSF, points to a different drug, called rapamycin; as Stipp explains, one way it appears to lengthen life is by slowing the production of the proteins needed for cell division. As more proteins are produced, so are more defective proteins, which can accumulate in cells and contribute to the symptoms we see as aging.

Though rapamycin has not gotten nearly the attention or money that sirtuins have, some put far more faith in its age-slowing effects. "I've been in this area for about 35 years, and I honestly have never thought that in my lifetime there would be something like a pill that you could take that would have this impact on aging," Arlan Richardson, director of the Barshop Institute for Longevity and Aging Studies at the University of Texas Health Science Center at San Antonio, says of the drug. Aging "may not be as intractable a problem as I thought," he says. Rapamycin even worked on adult mice equivalent in age to 60-year-old people.

So why isn't rapamycin more talked about? "The scientists involved with the rapamycin studies have been much less inclined to make bold claims," Kaeberlein says. "That may be in part due to the fact that the mouse rapamycin studies were done as part of [a government] testing program, so there's no commercial interest involved in selling a story." But if sirtuins and rapamycin don't work, researchers say, there are plenty of other possibilities to explore, from insulin signaling to mitochondrial function.

Stipp and others are confident that a "youth pill" is on the horizon—whether it comes from Sirtris or not. But some researchers are far less optimistic. Thomas Perls, for one, thinks it's reckless to suggest that science is anywhere close to such a drug. "I think people just don't get how incredibly complex aging is," says Perls, an associate professor of medicine at Boston University's School of Medicine, who for the last 16 years has run a study on centenarians. "Delivering the message that antiaging works, and that we're now in prime time in producing substances that work, is incredibly irresponsible." TR

KAREN WEINTRAUB IS A FREELANCE WRITER BASED IN CAMBRIDGE, MA. SHE IS THE FORMER DEPUTY HEALTH/SCIENCE EDITOR AT THE *BOSTON GLOBE*.



ENERGY

The German Experiment

THE GOVERNMENT SETS A PREMIUM PRICE ON SOLAR AND OTHER ALTERNATIVE POWER SOURCES. THE POLICY OFFERS LESSONS IN WAYS TO ENCOURAGE THE USE OF RENEWABLE ENERGY.

By EVAN I. SCHWARTZ

A decade ago, Germany launched a renewable-energy plan on an unprecedented scale. Its parliament, the Bundestag, enacted a law obligating the nation's electric utilities to purchase green power at sky-high rates—as much as 60 cents per kilowatt-hour for solar—under fixed contracts lasting up to 20 years. (German market prices for electricity, largely produced by coal and nuclear plants, were about 12 cents per kilowatt-hour.) The idea behind this "feed-in tariff" was that anyone would be able to build a renewable-power plant—or install rooftop solar panels—and be guaranteed predictable profits by feeding energy into the grid, where utilities would buy it at premium prices. The higher costs would be passed on as monthly surcharges to ratepayers, spread out among all homes and businesses in a country of about 80 million people. Fossil and nuclear fuels amount to "global pyromania," said Hermann Scheer, the German politician who championed the policy. "Renewable energy is the fire extinguisher."

THE RENEWABLE ENERGY SOURCES ACT
Passed by the German Bundestag February 25, 2000
Amended in 2004, 2008
www.bmu.de/english

Now, as the United States and other nations look toward creating their own policies for dealing with climate change, the effectiveness of the German experiment is a subject of debate. From one perspective, the Renewable Energy Sources Act of 2000 has exceeded its aims. Germany's first target was to get at least 10 percent of its electric power from renewable sources by 2010. The German grid now gets more than 16 percent of its electricity from these sources, and the government has raised its target for 2020 from 20 percent to 30 percent. The country avoided pumping about 74 million metric tons of carbon dioxide into the atmosphere in 2009. The German environment ministry also touts a side benefit: nearly 300,000 new jobs in clean power. As a result, the feed-in tariff has the support not only of the left-leaning politicians who originally backed it but also of most of the skeptics in the right-leaning parties that fought against it, says Claudia Kemfert, who heads the energy department at the German Institute for Economic Research in Berlin. "The skepticism is over," she says. "We're celebrating the success."

But from another perspective, the German policy is a government boondoggle. "It's not surprising that if you throw enough money at a certain technology, people will use it," says Severin Borenstein, codirector of the Energy Institute at UC Berkeley's Haas School of Business. Yes, the incentives triggered a frenzy of renewable-power installations, but at "very high prices," says Henry Lee, director of the Environment and Natural Resources Program at Harvard's John F. Kennedy School of Government. The spending on photovoltaics has been especially cost-inefficient in terms of producing power, Lee adds, because "Germany is the cloudiest country in Europe." Despite the weather, Germany now accounts for half the world's 20 gigawatts of installed solar capacity. "What that gets you," says Lee, "is high prices for electricity, locked in for 20 years, from technology that will be out of date within three years." Concludes Borenstein: "That's a failure of public policy."

As for the job-creation benefit, it may turn out to be ephemeral. Solar panels and wind turbines can be manufactured nearly anywhere in the world. Now, partly because of competition from low-cost manufacturing in China *(see "Solar's Great Leap Forward," p.52)*, many German manufacturers of this technology are struggling. Q-Cells, Conergy, and Solarworld have seen their stock lose much of its value since the start of 2008. Anton Milner, the founding CEO of Q-Cells, resigned in March after the company reported an annual loss of 1.36 billion euros ($1.67 billion). In May, to keep pace with the plunging cost of solar panels, the Bundestag cut the rates it set for selling solar power to the grid by 11 to 16 percent on top of a scheduled annual decrease of 10 percent. To try to compete with imports, solar companies have fired hundreds of workers, and the nation's solar trade association has warned of even more layoffs.

Meanwhile, some of the countries that copied key features of the German policy have also seen their booms start to fizzle. In 2008, Spain set an all-time record for photovoltaics, installing 2.46 gigawatts' worth of solar panels in a single year—41 percent of

LAIF/REDUX

all new installation worldwide, according to Solarbuzz, a research and consulting firm. But in Spain, buying all that high-priced power became a burden to the utilities. That, along with a longer contract term and aggressive pricing, caused the tariffs to be drastically cut. Without the high incentives, in 2009 Spain installed only 6 percent of the world's new solar-power capacity.

Nevertheless, interest in feed-in tariffs is growing in the United States. At least two cities—Sacramento, CA, and Gainesville, FL—have enacted local plans. California, Hawaii, and Vermont have passed laws that would create their own feed-in tariffs, and at least 15 other states have considered it.

What might these policies cost? In Germany, electricity prices have soared more than 60 percent over the past decade. But Germany's environmental ministry says the tariff system is responsible for less than a 10th of that increase, or about $3 per month for a typical household. Since German households consume about half as much electricity as U.S. homes, the extra cost for renewable energy has not been a deal-breaker for the public, says Kemfert, who contends that a majority of Germans support it. Overall, the tariff cost Germany an estimated $11 billion in 2008 alone, about a third of 1 percent of its GDP.

But why even bother with feed-in tariffs? Many economists favor either a carbon tax or a cap-and-trade system in which electricity plants buy permits to burn fossil fuel. "It would be better to tax brown power than subsidize green power," says Borenstein. Coal is the biggest carbon emitter among all energy sources, and it currently accounts for about half the electricity produced in the United States as well as in Germany. Phasing out coal should be the main goal, and pursuing that goal by putting a price on carbon, he says, allows the market to decide which renewable sources are most cost-effective. That's more efficient than letting the government set prices.

However, neither cap-and-trade nor a direct tax may be politically feasible in the United States. So would a national feed-in tariff be an acceptable alternative? Or would it also be politically doomed, since it, too, would raise electricity prices? To make a case for it, politicians would need to convince the American public that renewable power is worth it, pointing to Germany as the example. Indeed, the German experiment does show that a large industrial society can reach ambitious goals for scaling up new sources of clean electricity, with users paying the way. Germany expects to produce most of its electricity from renewable sources by 2030. Meanwhile, the United States produces only about 7 percent of its electricity from such sources, most of that from long-standing hydroelectric plants.

The real significance of the German plan, though, may not be as a model for other countries but as a source of permanent change in the world's energy economy. In this sense, Germany can be compared to early adopters of new gadgets, who often pay outrageous prices even though they know that others will get improved technology for much less a few years later.

Consider the changes in the market for wind power. By 2006, Germany had by far the largest wind-power base in the world, with 20.6 gigawatts of capacity. The massive scale brought the cost down, and wind began approaching grid parity in many parts of the world. In 2009, the United States and China were able to surpass Germany in capacity, but at far more attractive prices.

Thanks in part to the Germans, the same thing now appears to be happening in solar, with prices of photovoltaic panels plunging 40 percent last year alone. Yes, the critics are right that Germany's spending was wildly inefficient. But what Germany did was prime the global markets, showing that renewable technologies can be a big business worthy of investment. As a result, the United States may not need to copy Germany's experiment to reap the rewards. TR

EVAN I. SCHWARTZ IS AN AUTHOR AND JOURNALIST. HE PRODUCED AND COWROTE *SAVED BY THE SUN*, A PBS/*NOVA* DOCUMENTARY FEATURING A SEGMENT ABOUT THE GERMAN SOLAR POLICY.

What today's engineers, rocket scientists, and astrophysicists do for fun.





Exercise your skill, expand your mind, and challenge your creativity with everything from games to gadgets from Edmund Scientific.

For the latest trends in toys and technology, call for your free catalog or shop online at scientificsonline.com

Edmund Scientific's SCIENTIFICS®

1-800-728-6999 • www.scientificsonline.com



A WI-FI ANTENNAS

The iPad's two Wi-Fi antennas are designed for a strong signal—so strong that the device was, at first, banned from Israel because the country's ministry of communications feared it would interfere with other wireless frequencies. Testing proved that the iPad could adjust its signal without causing problems, and Israel lifted the ban.

B GPS AND CELLULAR ANTENNAS

GPS and cellular antennas make it possible to connect to AT&T's network, and the GPS allows for location-based applications such as turn-by-turn navigation and services that recommend local businesses.

C LED DISPLAY AND DRIVERS

Apple designed the iPad screen so that a user can easily view it from a variety of angles. The device uses a technology called in-plane switching, which aligns the molecules inside the screen in a way that gives it a wider viewing angle. The iPad also has an accelerometer that helps the device sense which end is up and switch the orientation accordingly.

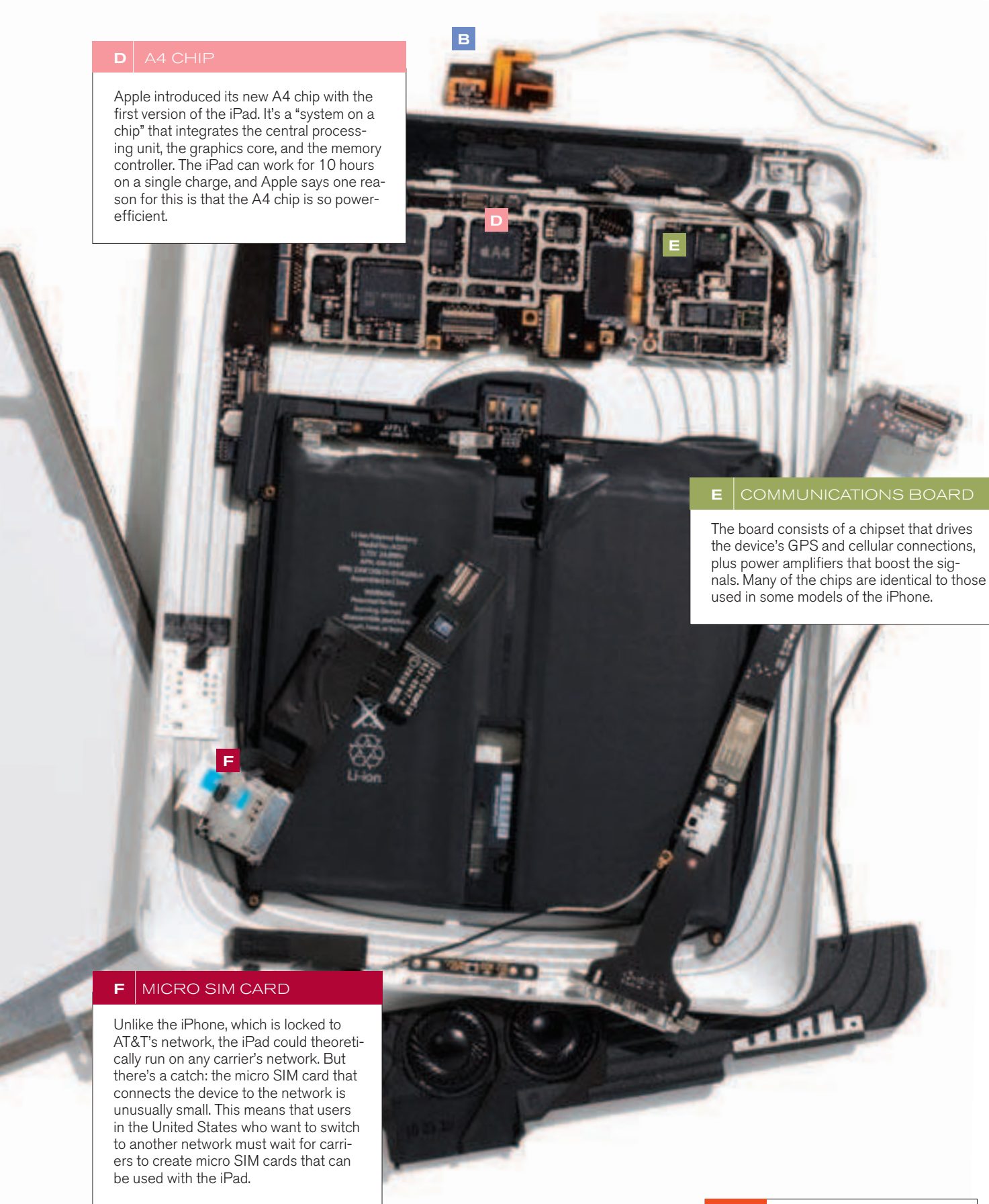
iPad 3G

A PEEK INSIDE THE TABLET REVEALS HOW IT CONNECTS TO THE WORLD

By ERICA NAONE

APPLE'S iPAD has revealed a huge market for tablet computers: more than two million units have sold since it went on sale in April. Before its launch, speculation was rampant that the new device would be an elaborate e-reader, but CEO Steve Jobs instead pitched the iPad as "the best browsing experience you've ever had." The 3G version indeed offers impressive connectivity, yet little inside it is radically innovative. Apple hasn't created amazing new tech so much as beautiful, well-integrated tech.

CHRISTOPHER HARTING



D A4 CHIP

Apple introduced its new A4 chip with the first version of the iPad. It's a "system on a chip" that integrates the central processing unit, the graphics core, and the memory controller. The iPad can work for 10 hours on a single charge, and Apple says one reason for this is that the A4 chip is so power-efficient.

E COMMUNICATIONS BOARD

The board consists of a chipset that drives the device's GPS and cellular connections, plus power amplifiers that boost the signals. Many of the chips are identical to those used in some models of the iPhone.

F MICRO SIM CARD

Unlike the iPhone, which is locked to AT&T's network, the iPad could theoretically run on any carrier's network. But there's a catch: the micro SIM card that connects the device to the network is unusually small. This means that users in the United States who want to switch to another network must wait for carriers to create micro SIM cards that can be used with the iPad.

www View an interactive version: **technologyreview.com/hack**

DEMO

Inexpensive, Unbreakable Displays

RESEARCHERS AT HP ARE SCALING UP A PROCESS FOR MAKING SILICON ELECTRONICS ON ROLLS OF PLASTIC.

By KATHERINE BOURZAC



1

Carl Taussig unfurls a roll of silvery plastic patterned with arrays of small iridescent squares, each a few centimeters across. The plastic in his hands, along with the scraps and scrolls of the material scattered on benchtops and desks in the rooms of Hewlett-Packard Labs in Palo Alto, CA, may look like silver wrapping paper, but each square contains thousands of silicon transistors. The transistors can switch pixels in displays on and off as fast as those in conventional flat-screen monitors and televisions, but they're far cheaper to fabricate and more resilient.

In today's displays, whether they're flat-panel TVs or iPads, the electronics that control the pixels are made of amorphous silicon on glass. Taussig's goal is to replace these heavy, fragile, expensive displays with lightweight, rugged, inexpensive ones made on plastic—without compromising performance. He is using high-volume roll-to-roll mechanics, the type of high-speed manufacturing process used in newspaper production, to make high-performance transistor arrays on the 33-centimeter-wide plastic rolls. HP researchers are now engineering a process for a planned pilot plant, where the company will produce the arrays at volumes of about 46,500 square meters a year through a partnership with Phicot, a manufacturer of thin-film electronics based in Ames, IA.

The idea is to combine these transistor arrays with flexible "frontplanes"—the part of a display that creates the images and that the transistors control. "Our goal is to make displays at a cost of $10 per square foot," Taussig says. That's about a 10th the price of today's displays. Silicon-on-plastic displays might be used in laptops, or a few thin sheets might be stuffed into briefcases, replacing printouts and pads of paper. Taussig also imagines "ginormous displays" pasted to walls to show videos and ads.

HP may not be the first company to market with a plastic display—Plastic Logic, which plans to release an e-reader soon, is likely to earn that distinction. But Plastic Logic's display isn't flexible—the plastic frontplanes and backplanes are protected by a rigid case. It also doesn't use silicon; it uses lower-performance organic transistors that aren't fast enough for video. HP hopes to gain an edge, Taussig says, by lowering the cost of the display while producing speedy, video-capable transistors.

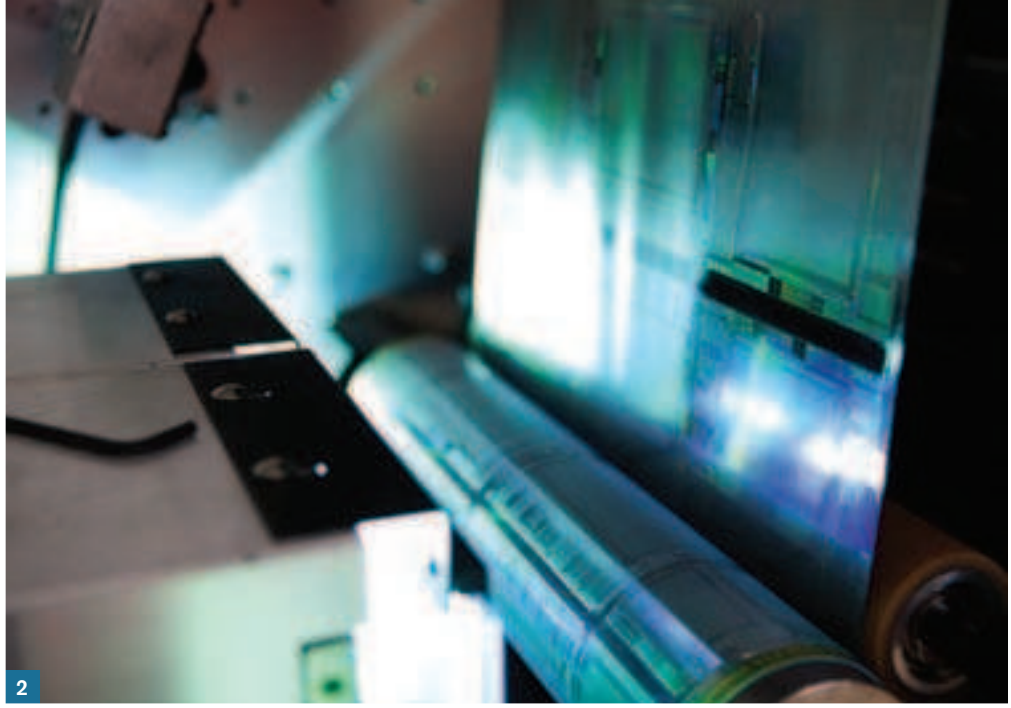
Part of the reason silicon-on-plastic displays haven't been produced before is that it's difficult to deposit high-quality silicon at temperatures low enough to avoid melting the plastic. Hewlett-Packard's partner, Phicot, has managed to solve that problem. HP has addressed another challenge: unlike glass, which provides a mechanically stable surface, plastic tends to distort. By finding a way to make nanoscale features on plastic, HP is opening the way to the large volumes and low costs that Taussig has in mind.

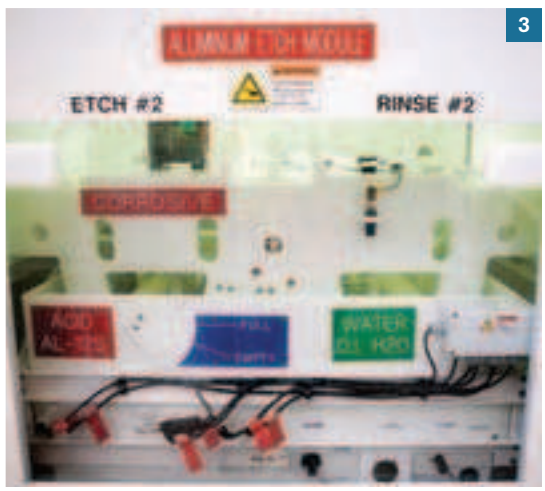
ON A ROLL

The key to forming nanoscale electronics on distortion-prone plastic is a process called self-aligned imprint lithography,

JEN SISKA







1. A researcher at Hewlett-Packard Labs holds a 33-centimeter-wide roll of plastic covered with amorphous-silicon transistor arrays designed to control pixels in displays. Each of the iridescent squares and rectangles—which vary in size to accommodate different test displays—contains hundreds to thousands of transistors. The plastic is 50 micrometers thick and is coated with multiple layers of silicon, metal, and other materials.
2. A cylindrical glass stamp presses against the film, creating a three-dimensional template used to pattern the device layers. As the plastic rolls over the stamp, it's cured with ultraviolet light (which appears bluish through a filter).
3. The film is then rolled through a series of chemical etching baths that alternately remove a layer of the template and carve into the metal. After a dip in chrome etchant (left), the plastic passes through a water rinse bath (right).

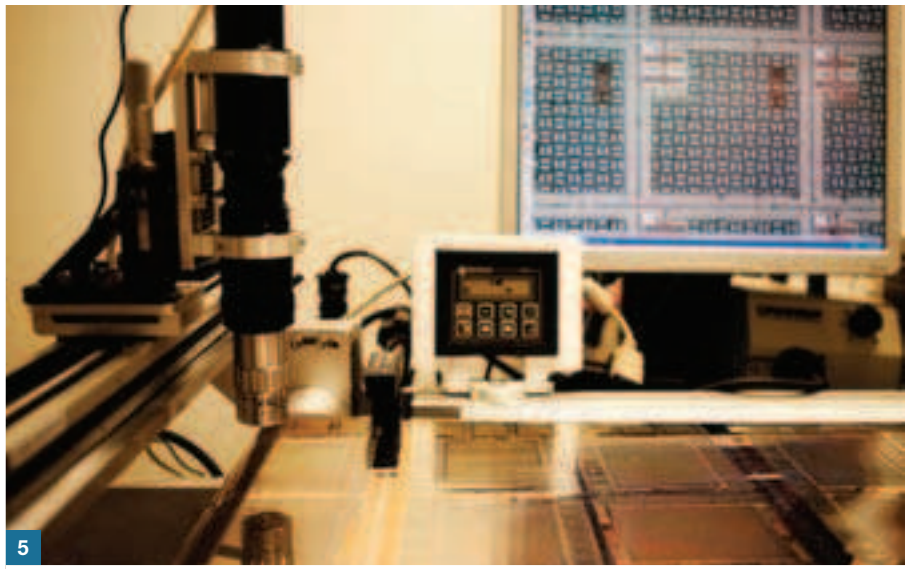
which Taussig's team invented in 2001, and which his group first applied to displays in 2006. Thin-film transistors have several layers, and in conventional manufacturing, the materials in each layer are deposited separately. After each layer is deposited, it's carved into precise patterns before the next layer is added. This process requires careful alignment of the photolithographic masks used to outline each pattern. Taussig's process, on the other hand, uses a single, three-dimensional template to pattern all the layers, eliminating the need to align different masks. "It's immune to distortion, which is the biggest challenge when making electronics roll-to-roll," Taussig says.

Researcher Albert Jeans shows off the starting material: a roll of plastic film coated with several thin layers of metal, amorphous silicon, and other materials needed to make the electronic circuits. To create the three-dimensional template, he loads the roll onto a spindle and threads it into a machine. The film moves through the machine, and a stationary blade spreads a uniform coating of liquid polymer over it. A stamp creates intricate impressions in the polymer coating, and these are instantly frozen in place by an ultraviolet light, which solidifies the polymer.

From the edge, the three-dimensional template that's been created resembles a microscopic city skyline. What follows is a series of etching steps, with the template controlling how far the underlying layers of metal and silicon are carved into at each one. Each step erodes the template uniformly, gradually eating into the thin films until the three-dimensional pattern of the polymer template is transferred to the layers below.

To start this carving process, the patterned plastic film is fed into a wet-etching machine. Once inside, the template is thoroughly coated with chrome etchant, which eats away roughly one micrometer from the entire surface. The thinnest parts of the template disappear, exposing parts of a thin film of metal below. Then the etchant carves into that exposed metal. The film is transferred to a plasma etching machine, which bombards the template with fluorine ions. They carve deeper into the film, this time cutting away parts of a silicon layer. Next it's back to the wet etcher to carve more metal layers. Each step carves







4. The roll is loaded into this vacuum chamber and passed through the silvery box at left. Inside, a plasma field blasts through the template to pattern the silicon layer. After the film exits through the bottom of the plasma etcher, it passes under an optical microscope (at the right of the image).
5. On this table, researchers record images of the transistors for inspection in a "display autopsy" if something goes wrong later on. The microscope image on the computer screen shows an individual pixel and its neighbors. The lines between the pixels bring in data and power.
6. A completed black-and-white display—made of a plastic-silicon backplane topped with an e-paper screen—is mounted under a video camera for testing. The blue cords connect to electrical contacts. The researchers monitor the display's performance as it repeatedly switches through a series of test images of the HP logo.

still further into the thin films of metal, insulating material, and silicon until parts of the bottommost layer of metal are exposed and etched, and the circuits are complete.

At each stage of the etching, Taussig uses a digital microscope to scan the surface for defects. He stores the images for examination during what he calls a "display autopsy." In that process, a computer screen shows rows and rows of transistors and capacitors interconnected with perpendicular conductive lines that will convey image data. These images also reveal subtle defects. The roll-to-roll process tolerates more variation than the processes for manufacturing traditional silicon electronics, but things can still go wrong.

If a transistor in the display doesn't work, the researchers can review the images and related data about the equipment settings (such as the tension on the roll, or the temperature) to identify the source of the problems: a faulty etching bath or a maladjusted spindle, for example.

To finish the display, researcher Hao Luo cuts a sheet of flexible "electronic paper," which contains microscopic black and white capsules; HP's transistors will control which capsules move to the surface of a pixel, making it appear black or white. He peels off the back of the e-paper to expose its adhesive and lays the material on top of the transistor array—a process about as simple as putting Scotch tape on a piece of paper, he says. This prototype is a step toward wristband displays that could show maps and other information to soldiers. The picture changes at a rate dictated by the e-paper, which is slow. But the electronics perform well enough to be combined with other, faster flexible pixel technologies. One leading candidate is a reflective, full-color, video-capable display that HP is developing.

As Taussig carries the finished rolls of plastic circuitry past rows of his colleagues' offices, he sees paper everywhere—internal motivational posters, comics, the usual stuff of cubicle walls. He envisions a day when the plastic he's carrying could replace them all. TR

www Watch video of HP's display printing process in action: **technologyreview.com/demo**

Calculus Is the Exploration of Two Basic Ideas. Master Them and Open a New World for Yourself!

Change and Motion: Calculus Made Clear, 2nd Edition, on DVD

One of the greatest achievements of the mind is calculus. It belongs in the pantheon of our accomplishments with Shakespeare's plays, Beethoven's symphonies, and Einstein's theory of relativity. Calculus is a beautiful idea exposing the rational workings of the world.

Calculus, separately invented by Newton and Leibniz, is one of the most fruitful strategies for analyzing our world ever devised. Calculus has made it possible to build bridges that span miles of river, travel to the moon, and predict patterns of population change. The fundamental insight of calculus unites the way we see economics, astronomy, population growth, engineering, and even baseball. Calculus is the mathematical structure that lies at the core of a world of seemingly unrelated issues.

Expanding the Insight

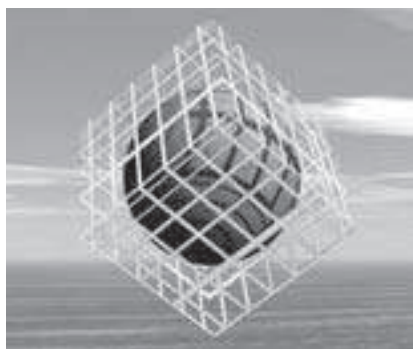
Yet for all its computational power, calculus is the exploration of just two ideas—the derivative and the integral—both of which arise from a commonsense analysis of motion. All a 1,300-page calculus textbook holds, Professor Michael Starbird asserts, are those two basic ideas and 1,298 pages of examples, applications, and variations.

Professor Starbird teaches that calculus does not require a complicated vocabulary or notation to understand it. "Calculus is a crowning intellectual achievement of humanity that all intelligent people can appreciate, enjoy, and understand."

This series is not designed as a college calculus course; rather, it will help you see calculus around you in the everyday world. Every step is in English rather than "mathese." The course takes the approach that every equation is also a sentence that can be understood, and solved, in English.

About Your Professor

Professor Michael Starbird is a distinguished and highly popular teacher with an uncommon talent for making the wonders of mathematics clear to nonmathematicians. He is Professor of Mathematics and



© Digital Stock.

a Distinguished Teaching Professor at The University of Texas at Austin. Professor Starbird has won several teaching awards, most recently the 2007 Mathematical Association of America Deborah and Franklin Tepper Haimo National Award for Distinguished College or University Teaching of Mathematics, which is limited to three recipients annually from the 27,000 members of the MAA.

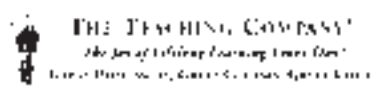
About The Teaching Company®

We review hundreds of top-rated professors from America's best colleges and universities each year. From this extraordinary group we choose only those rated highest by panels of our customers. Fewer than 10% of these world-class scholar-teachers are selected to make The Great Courses®.

We've been doing this since 1990, producing more than 3,000 hours of material in modern and ancient history, philosophy, literature, fine arts, the sciences, and mathematics for intelligent, engaged, adult lifelong learners. If a course is ever less than completely satisfying, you may exchange it for another, or we will refund your money promptly.

Lecture Titles

1. Two Ideas, Vast Implications
2. Stop Sign Crime—The First Idea of Calculus—The Derivative
3. Another Car, Another Crime—The Second Idea of Calculus—The Integral
4. The Fundamental Theorem of Calculus
5. Visualizing the Derivative—Slopes
6. Derivatives the Easy Way—Symbol Pushing
7. Abstracting the Derivative—Circles and Belts
8. Circles, Pyramids, Cones, and Spheres
9. Archimedes and the Tractrix
10. The Integral and the Fundamental Theorem
11. Abstracting the Integral—Pyramids and Dams
12. Buffon's Needle or π from Breadsticks
13. Achilles, Tortoises, Limits, and Continuity
14. Calculators and Approximations
15. The Best of All Possible Worlds—Optimization
16. Economics and Architecture
17. Galileo, Newton, and Baseball
18. Getting off the Line—Motion in Space
19. Mountain Slopes and Tangent Planes
20. Several Variables—Volumes Galore
21. The Fundamental Theorem Extended
22. Fields of Arrows—Differential Equations
23. Owls, Rats, Waves, and Guitars
24. Calculus Everywhere



About Our Sale Price Policy

Why is the sale price for this course so much lower than its standard price? Every course we make goes on sale at least once a year. Producing large quantities of only the sale courses keeps costs down and allows us to pass the savings on to you. This also enables us to fill your order immediately: 99% of all orders placed by 2 pm eastern time ship that same day. Order before September 14, 2010, to receive these savings.



SAVE $185!
OFFER GOOD UNTIL SEPTEMBER 14, 2010

1-800-TEACH-12 (1-800-832-2412)
Fax: 703-378-3819

Special offer is available online at
www.TEACH12.com/5tech

The Great Courses
THE TEACHING COMPANY
4151 Lafayette Center Drive, Suite 100
Chantilly, VA 20151-1232

Priority Code 40329

Please send me **Change and Motion: Calculus Made Clear, 2nd Edition**, which consists of twenty-four 30-minute lectures plus Course Guidebooks.

☐ **DVD $69.95** (std. price $254.95) **SAVE $185!**
plus $10 shipping, processing, and Lifetime Satisfaction Guarantee

☐ **Check or Money Order Enclosed**

* Non-U.S. Orders: Additional shipping charges apply. For more details, call us or visit the FAQ page on our website.

** Virginia residents please add 5% sales tax.

Charge my credit card:

☐ VISA ☐ ☐ ☐

Account Number _____ Exp. Date _____

Signature _____

Name (please print) _____

Mailing Address _____

City/State/ZIP _____

Phone *(If we have questions regarding your order—required for international orders)* _____

☐ **FREE CATALOG.** Please send me a free copy of your current catalog (no purchase necessary).

Special offer is available online at www.TEACH12.com/5tech
Offer Good Through: September 14, 2010

FROM THE LABS

MATERIALS

A Memory and Logic Device

HP RESEARCHERS DEMONSTRATE LOGIC WITH MEMRISTORS

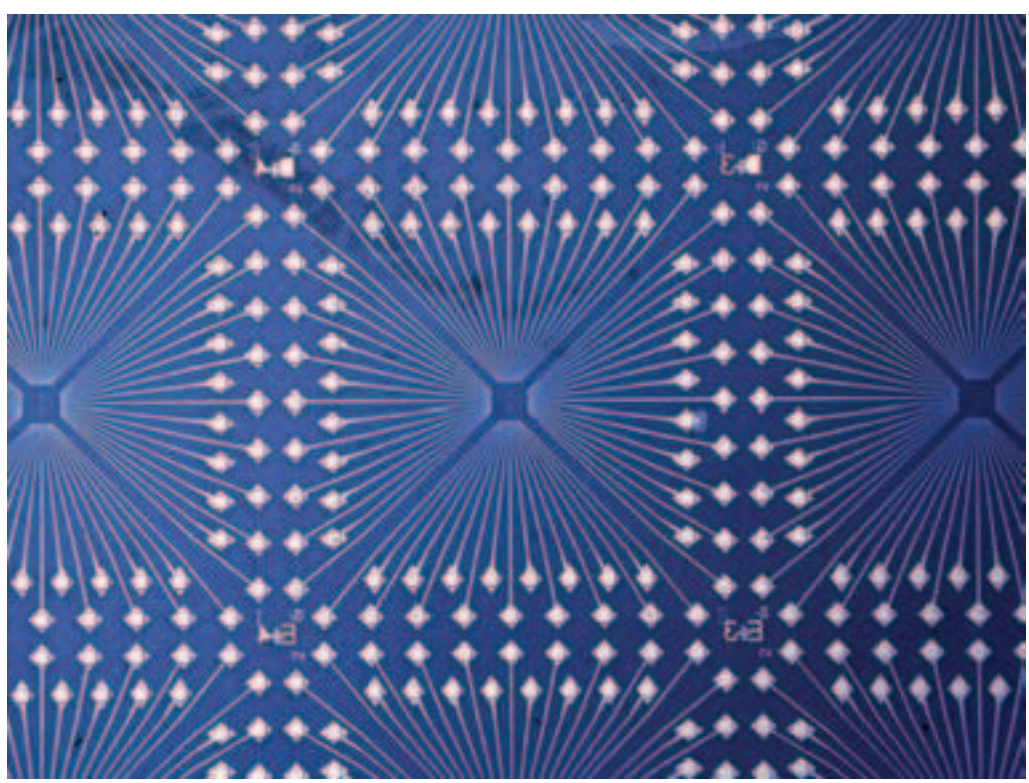
SOURCE: "'MEMRISTIVE' SWITCHES ENABLE 'STATEFUL' LOGIC OPERATIONS VIA MATERIAL IMPLICATION"
R. Stanley Williams et al.
Nature 464: 873–876

Results: Researchers at Hewlett-Packard have shown that nanoscale circuit elements called memristors, which have previously been made into memory devices, can perform full Boolean logic, the type used for computation in computer processors.

Why it matters: Memristor logic devices are about an order of magnitude smaller than devices made from transistors, so they could pack more computing power into a given space. Memristor arrays that perform both logic and memory functions could eliminate the need to transfer data between a processor and a hard drive in future computers, which would save energy.

Methods: HP researchers fabricated memristors of various sizes on a silicon substrate by growing metal nanowires, coating them with titanium dioxide, and topping them with another series of metal nanowires oriented perpendicular to the first group. A memristor is formed where the two layers of wires cross. Each wire was connected to some test circuitry that the researchers used to bring current into the system. Using this test system, the researchers showed that a pair of memristors could serve as a logic gate: it processed information by switching one of the memristors on or off to create a *1* or a *0*, depending on the initial states of the two elements. The memristors could also serve as a "latches"—that is, they retained data, "remembering" whether they had recently switched to a *1* or a *0*.

Next steps: The basic material properties of the metal oxides used to make memristors are still not well understood, so it's not clear whether the devices will be as reliable as silicon transistors. HP Labs researchers are working toward introducing a memory product based on memristors in 2013, and researchers will learn more as they develop facilities to make them.



LOGIC TEST Arrays of memristors located where these electrical contacts converge can perform logic and memory functions.

WEI WU

Black Silicon

A SIMPLE, INEXPENSIVE TREATMENT COULD REDUCE THE COST OF SOLAR POWER

SOURCE: "EFFICIENT BLACK SILICON SOLAR CELL WITH A DENSITY-GRADED NANOPOROUS SURFACE"
Howard Branz et al.
Applied Physics Letters 95:123501–123503

Results: A simple chemical technique can create a highly antireflective surface on silicon solar cells. The new method for making this so-called "black silicon" results in

cells that convert 16.8 percent of the light that hits them into electricity, which is comparable to the efficiency of many commercial solar cells. It's a significant improvement over the previous record for solar cells made of black silicon, which was 13.9 percent.

Why it matters: The technique could make crystalline solar cells, the most common type, cheaper to make, because it is less expensive than producing the antireflective coatings now used to keep photons from bouncing off the cells and going to waste. Previously developed methods for making black silicon may be impractical for large-scale manufacturing because they are more complex or involve slow and costly equipment. The new research demonstrates that the antireflective surface can be readily made using equipment already on hand at solar-cell factories.

Methods: The researchers submerged a silicon wafer in an acidic solution containing trace amounts of gold. Chemical reactions generated gold nanoparticles, which then catalyzed reactions that etched holes of varying depths into the wafer. This created a porous structure that blurs the boundary between the surrounding air and the bulk silicon, reducing reflection.

Next steps: The researchers are working to increase the cell efficiencies further and performing more detailed calculations to determine how the process will affect the cost of solar power.

INFORMATION TECHNOLOGY

Automated Towel Folder

A ROBOT LEARNS TO RELIABLY MANIPULATE FLEXIBLE OBJECTS

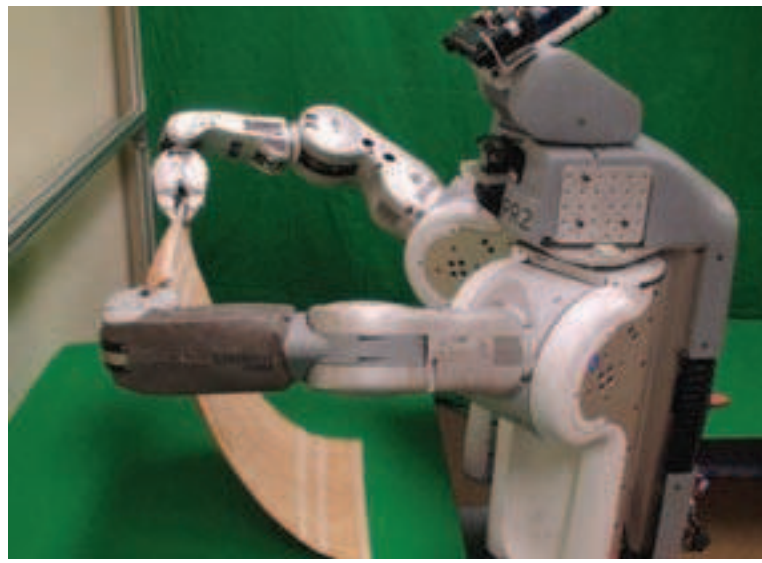
SOURCE: "CLOTH GRASP POINT DETECTION BASED ON MULTIPLE-VIEW GEOMETRIC CUES WITH APPLICATION TO ROBOTIC TOWEL FOLDING"
Jeremy Maitin-Shepard et al.
2010 IEEE International Conference on Robotics and Automation (ICRA2010), May 3–8, 2010, Anchorage, AK

Results: For the first time, a robot can reliably sort, fold, and stack different-sized towels that it encounters in a disordered pile. Previous robots have had only limited success at folding towels, even when the towels were laid out in a particular orientation and the robots were programmed with their dimensions.

Why it matters: Even robots that are adept at manipulating rigid objects, such as cups or tools, have not been able to dependably handle unfamiliar objects made of cloth, which changes shape. The ability to do so could eventually allow robots to help with laundry or other tasks that involve malleable objects.

Methods: After the robot picks up a towel from a pile, it rotates the towel with a two-fingered gripper and uses high-resolution cameras to view it from multiple angles. An algorithm developed by researchers at the University of California, Berkeley, enables the robot to distinguish the towel's edges from folds in the cloth by estimating the curvature of the cloth (an edge is slightly sharper than a fold). By noting where two edges meet, it can identify a corner. After grasping the corner, it identifies and grasps an adjacent corner; then it untwists the towel and checks its configuration before folding it. To keep it from getting stuck, the researchers designed a self-correcting process. If it detects an error, it attempts to correct it or, if necessary, drops the towel and starts over. The robot successfully folded towels on its own 50 out of 50 times.

Next steps: The robot currently takes about 20 minutes to fold a single towel; the researchers are adapting the algorithm to speed up the process. They also plan to program robots to fold other objects, such as shirts, and to learn how to fold new items after observing a human demonstration.



FOLD, REPEAT This PR2 robot from Willow Garage in Menlo Park, CA, has been programmed to use twin high-resolution cameras to examine a towel before folding it. It started by pulling this towel from a disordered pile.

JEREMY MAITIN-SHEPARD AND PIETER ABBEEL

Uncovering Search Histories

PERSONALIZED SERVICES ON THE INTERNET NEED HIGH LEVELS OF SECURITY

SOURCE: "PRIVATE INFORMATION DISCLOSURE FROM WEB SEARCHES (THE CASE OF GOOGLE WEB HISTORY)"
Claude Castelluccia et al.
Proceedings of the 10th Privacy Enhancing Technologies Symposium, July 21–23, 2010, Berlin, Germany

Results: Researchers successfully reconstructed the Web search histories of specific Google users by stealing the users' credentials and impersonating them. They were able to identify about 65 percent of what the users

had been searching for, and they could tell whether a user had searched for a particular term.

Why it matters: Personalized Web services can help make searches and other tasks faster, but the new research suggests that they could also be used to collect information about search histories that people might prefer to keep private. A single search on a public Wi-Fi network would be enough to expose a person's search history to a potential attacker. Although Google has made changes to prevent search histories from being discovered, the researchers say that other search engines are likely to have similar vulnerabilities. They recommend that Web applications encrypt all searches and credentials.

Methods: Google encrypts sensitive information such as passwords, but it doesn't encrypt the authentication credentials that it uses to identify particular users of its search service. By intercepting these credentials, the researchers were able to impersonate a given user. Then they performed automated test searches in the user's name and pieced together the Web search history from the personalized recommendations that Google provided.

Next steps: The researchers plan to analyze other search engines for similar leaks. They also continue to track the progress at fixing the problems they found.

BIOTECHNOLOGY

Rejuvenating the Brain

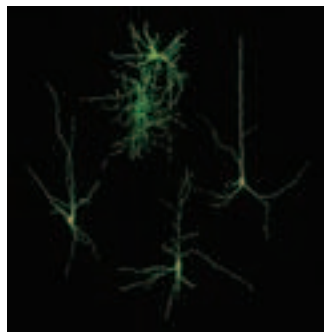
NEURONS TRANSPLANTED FROM FETAL ANIMALS MAKE OLDER BRAINS ACT YOUNG

SOURCE: "CORTICAL PLASTICITY INDUCED BY INHIBITORY NEURON TRANSPLANTATION"
Arturo Alvarez-Buylla, Michael P. Stryker, Sunil P. Gandhi, et al.
Science 327: 1145–1148.

Results: By transplanting fetal neurons into young mice, researchers induced the animals to rewire neural circuits in their visual system.

Why it matters: Rodents and other animals, including humans, experience a period of neural plasticity before the brain circuitry becomes fixed. Researchers hope to enhance this innate capacity in order to improve healing after brain injury and other neurological problems in adulthood. This study was the first to show that animals can be induced to undergo a second round of flexibility. Pinpointing the specific molecules that made it possible could inspire new treatments.

Methods: The researchers took neurons of a specific type, called inhibitory neurons, from the brains of fetal mice and grafted them into newborn or young mice. Then they gauged neural plasticity by measuring changes in the animals' brains after they were blinded in one eye. The mice experienced the normal period of neural flexibility in the visual system at around 28 days. But a second period of plasticity occurred at around 35 days, when the visual circuitry is normally fixed. Its timing corresponded to the age of the transplanted cells, which suggests that the transplant triggered it.



LIMBERED UP The neurons shown here, transplanted from an embryo into the brain of a young mouse, help the brain adapt.

Next steps: Researchers plan to isolate specific types of inhibitory neurons and transplant them in an attempt to find the specific cell type responsible.

Anti-Cancer RNA

PARTICLES TARGET RNA INTERFERENCE TO TUMOR CELLS

SOURCE: "EVIDENCE OF RNAi IN HUMANS FROM SYSTEMICALLY ADMINISTERED siRNA VIA TARGETED NANOPARTICLES"
Mark E. Davis et al.
Nature 464: 1067–1070

Results: Researchers at Caltech used specialized nanoparticles to deliver a type of gene-silencing RNA to cancer cells in human subjects. Biopsies from three melanoma patients who had been given the therapy showed that the particles entered cancer cells but not healthy cells, and that the RNA successfully blocked the action of a cancer-related molecule that was its target.

Why it matters: Certain RNA molecules can cut messenger RNA and prevent it from producing proteins, a phenomenon known as RNA interference. But it has been difficult to deliver RNA-based therapies into the right cells. RNA injected into the bloodstream is typically filtered out by the kidneys before reaching its target, so the therapy has been limited to areas where the molecules can be delivered directly, such as the eyes or lungs. The new trial is the first to show that RNA can be ferried through the bloodstream in nanoparticles that protect the molecules and deliver them to cancer cells.

Methods: Researchers started with an RNA molecule designed to silence a gene used for DNA synthesis and repair. They enclosed the RNA in nanoparticles made of a sugar-based polymer, another polymer that binds weakly to water to enhance the particles' stability, and a protein that is displayed on the particles' exterior and binds with receptors on cancer cells, signaling the cells to absorb them. Once inside those cells, the nanoparticles release the RNA molecules to attack their targets.

Next steps: Researchers are studying patients with other tumors in an early-stage trial. They won't be able to assess how effective the treatment is at shrinking tumors until testing it in more patients. TR

COURTESY OF DEREK SOUTHWELL



IMAGES OF INNOVATION

82 full-color pages of *Technology Review's* most exciting visual technology stories from the past year.

ONLY $9.95!
+ TAX & S/H



To order call 1.800.877.5230 (8AM TO 8PM ET) or online at www.technologyreview.com/ioi

Alumni-to-Alumni Directory & Classifieds

TIAX LLC

EXCELLENT JOB OPENINGS FOR OUTSTANDING PROFESSIONALS

We in-source promising early-stage technologies and,
in our extensive laboratories and facility,
transform them to scale-up-ready technologies for industry.
www.tiaxllc.com

We are headquartered at 35 Hartwell Avenue, Lexington, MA,
in a premier technology corridor.

At our Lexington location, we are hiring:

- Mechanical engineers
- Advanced materials engineers and scientists
- Chemical engineers and electrochemists

In three programs:

- BS graduates for two- to three-year internship and apprenticeship (excellent experience for those preparing for graduate degrees)
- Postdoctoral fellows for one or two years, for those who want to operate at the intersection of academia and industry
- Engineers and scientists with relevant experience to join our core staff

We cherish and promote talent, excellence, and impact.

To apply, please send résumés in confidence to careers@tiaxllc.com.

RECRUITMENT

EDELMAN & ASSOCIATES

Insight and Innovation in Executive Search and Technical Recruiting

Finding technical and management talent for software,
financial services, and other technology-driven companies

Paul Edelman '78
paul@edeltech.com
508-947-5300

To see a listing of current searches, please visit us at www.edeltech.com.

For confidential consideration, send your résumé to paul@edeltech.com.

GENTLEMEN

The smart money is on smart women. Date a few.

www.rightstuffdating.com
800-988-5288

Upcoming Events

EMTECH@MIT 2010
10th Anniversary Event
September 21-23, 2010
MIT Campus, Cambridge, MA
www.technologyreview.com/emtech

2010 IEEE CONFERENCE ON INNOVATIVE TECHNOLOGIES FOR AN EFFICIENT AND RELIABLE ELECTRICITY SUPPLY
September 27-28, 2010
Waltham, Massachusetts
www.ieee-energy.org

USA Science & Engineering Festival
October 23-24, 2010
Washington, D.C.
www.usasciencefestival.org

2010 Medical Innovation Summit
November 1-3, 2010
Cleveland, OH
www.clevelandclinic.org/innovations/summit

The conference that brings you the future of technology.

SPECIAL DISCOUNT
FOR
TECHNOLOGY REVIEW
SUBSCRIBERS!

Learn more at:
www.technologyreview.com/emtech

EmTech@MIT
MIT CAMPUS • CAMBRIDGE, MA
SEPTEMBER 21-23, 2010



The Long Fight Ahead

WHEN RESEARCHERS FOUND THE CAUSE OF AIDS IN THE EARLY '80S, THEIR WORK HAD ONLY JUST BEGUN

By MATT MAHONEY

By early 1984, the Reagan administration had spent three years being accused of inaction on AIDS—ever since the Centers for Disease Control first began tracking cases. Now the administration was keen to trumpet its progress.

To have heard Margaret Heckler tell it at her April 23 news conference, it was all over but the shouting. Only a year earlier, said the secretary of health and human services, she had "made the conquest of AIDS the federal government's number-one priority." And now not only had the "probable cause" of acquired immune deficiency syndrome been found; it had also become possible—thanks to a newly developed blood test—to identify AIDS victims and AIDS-tainted blood "with essentially 100 percent certainty." And to top this dazzling array of accomplishments, Heckler announced that a preventive vaccine should be "ready for testing in approximately two years."

Science journalist Judith Randal, in a column for *TR*, had her doubts:

Not so fast, madam secretary. The truth is that the cause of AIDS may or may not have been found. And there is no evidence that anything discovered to date will make a dime's worth of difference to people who already have AIDS or get it in the next few years. Even the blood test is not yet a fait accompli. And as for the vaccine, only the wildest of optimists expect it to be a reality before the end of the decade.

Heckler was right about researchers' having identified the cause of AIDS, but that was far from clear at the time. National Institutes of Health researcher Robert Gallo had identified a virus that he called HTLV-III, and a French group led by Luc Montagnier had found one dubbed LAV a year earlier. They were the same virus (it was renamed HIV in 1986), but the competing claims would not be sorted out until 1987, when the researchers grudgingly shared credit—and royalties on the patent for the blood test, which the U.S. Food and Drug Administration approved in 1985.

Meanwhile, as Randal pointed out, Heckler's predictions about a vaccine were wildly overoptimistic, mostly because of the nature of the viruses that researchers were focusing on.

Although we don't know precisely which virus is responsible for AIDS, scientists are fairly certain that the disease involves a special class of viruses, known as retroviruses (to which both HTLV-III and LAV belong). The genes of most viruses are made of DNA, which then makes RNA. But in retroviruses the reverse occurs, and the genes are made of RNA, which then makes DNA.

Making a vaccine for a virus—let alone a retrovirus—is difficult and time consuming. The virus must be grown in laboratory culture and used intact to make a product that will generate antibodies, the molecules in the body's immune system that attack foreign substances. To make sure the vaccine won't cause the disease, weakened or dead strains of the virus must be developed. ...

SLOW BURN In 1984, some thought an AIDS vaccine was only a few years away.

Once (and if) that is accomplished, animal tests must then be conducted to show that the AIDS virus actually causes the disease, and that the vaccine is capable of safely neutralizing it. Human field trials are also required before the vaccine can be widely used. All this suggests that an AIDS vaccine is probably six to eight years away

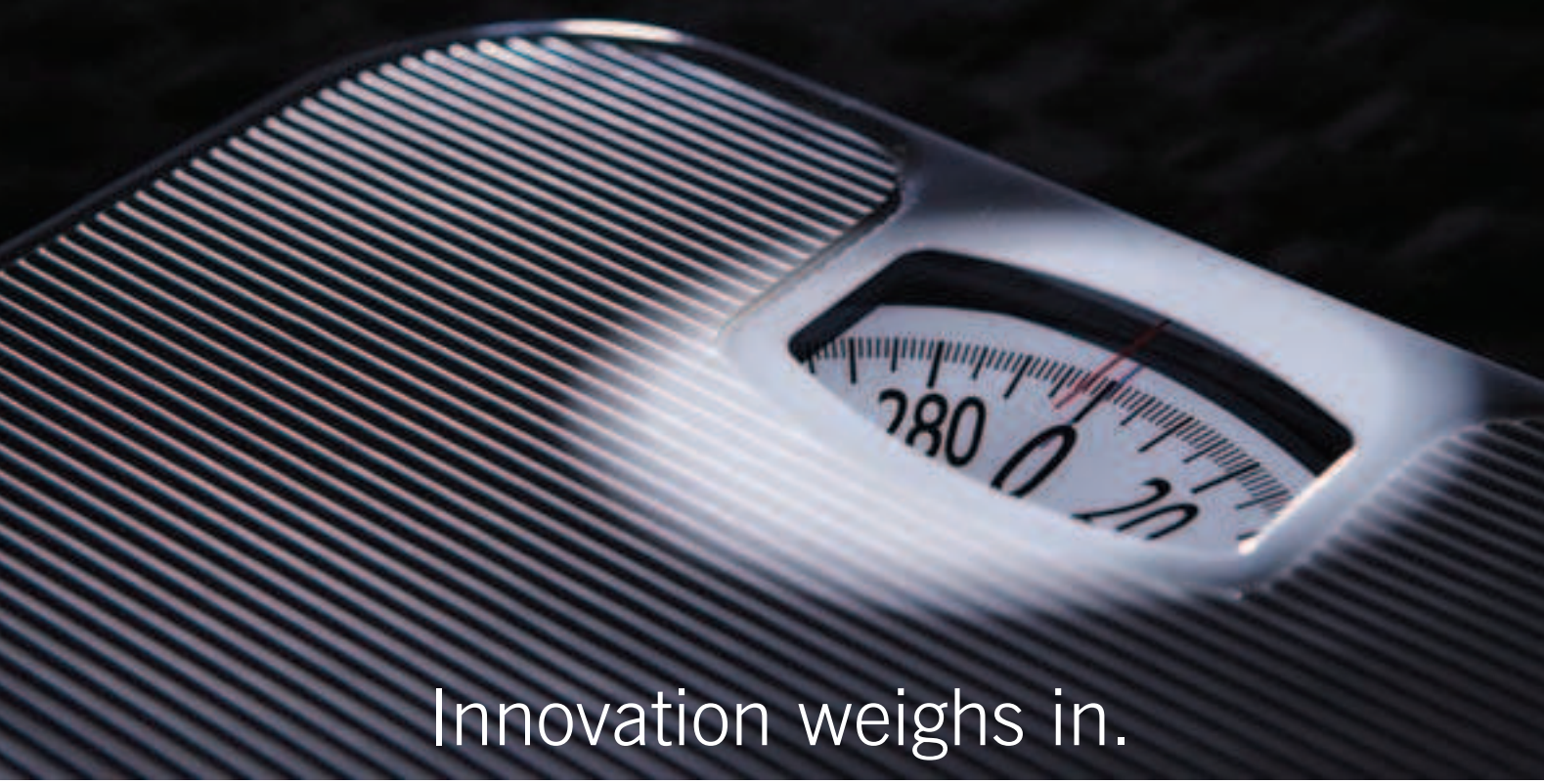
Obviously, Randal was being overly optimistic about a vaccine herself. But she advocated trying to help those already affected, an approach that many researchers take today *(see "Can AIDS Be Cured?" p. 44)*.

In the meantime, no one is known to have recovered from AIDS, and the problem is not going away. The number of cases continues to double about every six months, and because the incubation period is so long, a lot more cases are certainly in the pipeline. Since more than 4,600 AIDS patients have been diagnosed in the United States alone, that means there could well be 100,000 or more in this country before the end of the decade.

Granted, treatment may very well have improved by that time. But this, too, is unpredictable. A year ago researchers held great hope for one type of interferon as well as a drug called interleukin two. However, neither medication is panning out. With a disease as complex as this one, the light at the end of the tunnel has a nasty habit of flickering brightly and then going dim. TR

ANTHONY RUSSO

Technology Review (ISSN 1099-274X), Reg. U.S. Patent Office, is published bimonthly by the Massachusetts Institute of Technology. Entire contents ©2010. The editors seek diverse views, and authors' opinions do not represent the official policies of their institutions or those of MIT. Printed by Brown Printing Company, Waseca, MN. Periodicals postage paid at Boston, MA, and additional mailing offices. Postmaster: send address changes to Technology Review, Subscriber Services Dept., PO Box 16327, North Hollywood, CA 91615, or via the Internet at www.technologyreview.com/customerservice. Basic subscription rates: $39 per year within the United States; in all other countries, US$52. Publication Mail Agreement Number 40621028. Send undeliverable Canadian copies to PO Box 1051 Fort Erie, ON L2A 6C7. Printed in U.S.A.
ABC audited



Innovation weighs in.

November 1-3, 2010

What's the BIG deal about obesity? It is not just body mass—it is cancer, coronary disease, stroke, sleep apnea, erectile dysfunction, and many more comorbidities. This pandemic is reshaping America.

Be part of the technological revolution that is responding to this national crisis—it will save lives, improve health, and create new wealth.

Register today: **www.ClevelandClinic.org/summit**

Use promotional code **TECHNOLOGY** and
pay $649 until August 15, 2010.

2010 Medical Innovation Summit
Obesity, Diabetes & the Metabolic Crisis

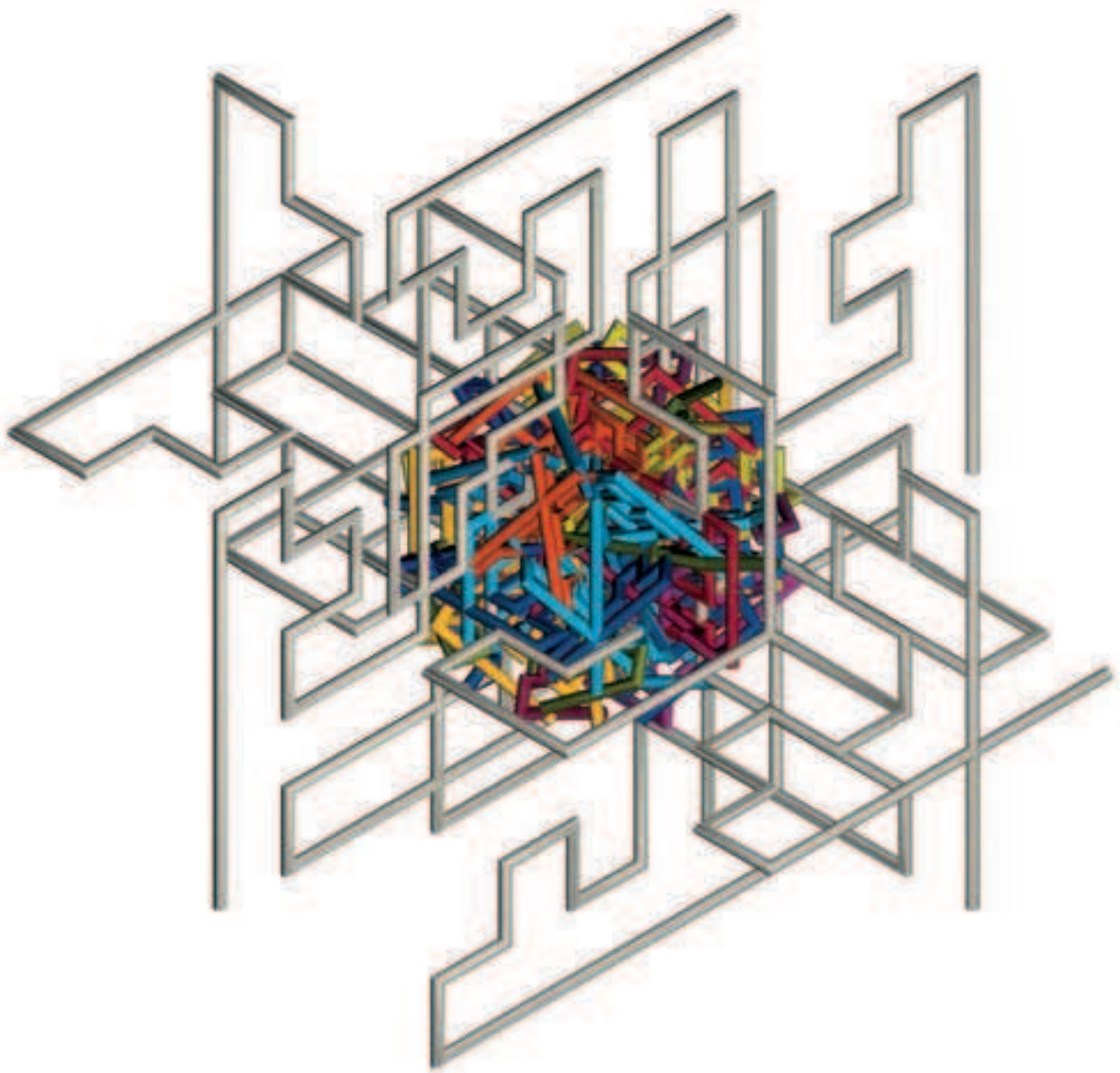
Cleveland Clinic

Smarter technology for a Smarter Planet:

Why the old ways of working aren't working.

On a smarter planet, technology has made us more connected, but not necessarily more productive. As new global opportunities emerge, companies are finding that their internal processes aren't as dynamic as the marketplace requires. In fact, employees spend up to 25% of their time just looking for information that should be readily available to them. Managers require visibility across their company in order to make fast, informed decisions. IBM can help optimize business processes to align with the way people actually work and provide a contextual, information-rich environment. By combining elements of business process management, collaboration and SOA solutions, employees can act on real-time insights and locate the right people to seize new opportunities—helping to reduce costs.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/connected



IBM, the IBM logo, ibm.com, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. © International Business Machines Corporation 2010.